TABLE OF CONTENTS

SECTION **PAGE**

LIST OF FIGURES

FIGURE **PAGE**

LIST OF TABLES

TABLE **PAGE**

5.4 INFORMATION ASSURANCE REQUIREMENTS

5.4.1 Section Overview and Scope

This UCR section originally addressed the Information Assurance requirements for ~~es~~ VVoIP components. ~~but~~While VVoIP Information Assurance remains the primary focus, this section has ~~recently~~ been expanded to incorporate the Information Assurance requirements for additional UC APL products. This section of the UCR now incorporates the Information Assurance requirements for Security Devices which are defined further ~~further~~ in Section 5.8. However, note that the functional requirements for Security Devices can still be found in UCR Section 5.8. In this context Security Devices ~~consist~~include ~~of~~ Firewalls, Intrusion Detection/Prevention Systems, and Virtual Private Network servers. Per recent decisions from the UC Steering Group, additional products will be added to this category of devices in the future as well. ~~In addition~~Lastly, this section has been augmented to address the requirements for End Instruments which reside on mobile smartphone platforms, termed "Smartphone End Instruments.~~,~~"

The first phase associated with merging Information Assurance requirements from Section 5.8 has been completed. This initial phase focused mainly on providing a one-for-one mapping of requirements extracted from 5.8 and incorporated to this section in order to minimize impact to any associated test plans. A follow-on phase will further merge those Security Device Information Assurance requirements that share close similarity with the Information Assurance requirements specified for VVoIP components. ~~have been incorporated into this section. Information Assurance requirements The TDM switch Information Assurance requirements have beenwere removed from this section in UCR 2008 Change 1 due to the removal of the TDM switch requirements from UCR 2008 Change 1 Section 5.2.~~

5.4.2 VVoIP Information Assurance Requirements Structured Process

This section provides an overview of the VVoIP Information Assurance design and specifies the VVoIP Information Assurance requirements using a defined, structured process in order to secure the VVoIP system. The process is called the Information Assurance Process, shown in Figure 5.4.2-1, because it applies to any Information Assurance design. A basic tenet of this process is that threats are the primary driver for all stages of the Information Assurance Process. However, it is recognized that architectures may be influenced by other drivers, such as political, time, and technical motivators. This section is structured to follow the Information Assurance Process in the development of the VVoIP Information Assurance design and requirements.

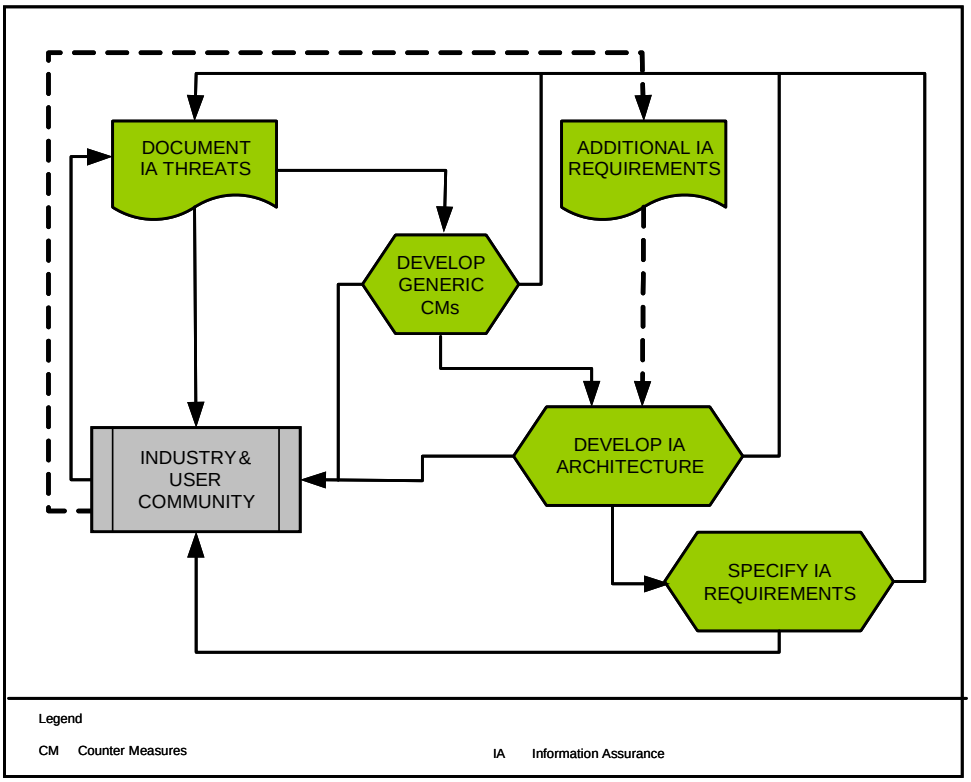

Figure 5.4.2-1. Information Assurance Process

The first step in the Information Assurance process is to document the threats based on a preliminary understanding of how the system will be deployed and in conformance with the DoD high-level Information Assurance requirements. A summary of the threats is provided in this UCR section, but the details of the threats are found in the "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment," Version 3.4, DoD RTS Information Assurance Working Group, 22 May 2009. In creating the Information Assurance section of the UCR, the threats were vetted with industry and the user community in order to get user buy-in and to ensure that all known threats were documented. An example of a threat is eavesdropping on the media stream of a telephone call to hear the contents of a conversation. After the threats were documented, the risks associated with each threat were classified based on the likelihood of a successful attack and the impact of a successful attack. The classification of the risks permitted the prioritization of resources to mitigate the risks during the development of the Information Assurance design.

Based on the threats, a set of generic countermeasures (CMs) was developed. A summary of the CMs is discussed in the main body of UCR, but the details of the CMs are found in "DoD RTS Information Assurance Countermeasures," Version 0.7, DoD RTS Information Assurance Working Group, 29 March 2006. The reason generic CMs were developed, instead of specific CMs, is that it allows for maximum flexibility in selecting an approach to implement the countermeasure. Encryption of the media stream is an example of a generic countermeasure,

which would mitigate the threat associated with eavesdropping on the media stream. In defining the generic CMs, it is important to understand the interdependence of the CMs and document those interdependencies.

For example, confidentiality without authentication and authorization diminishes its benefit. In addition, it is important to map threats to CMs to ensure all threats are addressed. As with the threats, the generic CMs were vetted with industry and the user community to determine if they were feasible and to get user buy-in.

The next step was to develop an Information Assurance design based on the generic CMs and threats. The first step in the development of the Information Assurance design was to identify candidate mechanisms that satisfy the CMs and mitigate the threats. For example, confidentiality of the bearer stream could be achieved by implementing the SRTP, IPSec, or Type 1 point-to-point bulk encryption. The candidates were vetted with the user community and industry before selecting the default solution(s) for the Information Assurance design. Alternative solutions were allowed in specific cases, but a default solution was specified to ensure multivendor interoperability. In addition, although the threats and generic CMs were the primary driver of the Information Assurance design, political, time, and technical motivators also influenced the Information Assurance design and requirements and were incorporated into the Information Assurance design.

After the design was completed, the final step in the Information Assurance Process involved documenting the requirements necessary to achieve the Information Assurance design in a multivendor interoperable integrated environment that could be tested. An example of a requirement is that the system shall use SRTP for encrypting the media stream. As with the threats and CMs, the requirements were vetted with industry and the user community to ensure that the requirements were clear, concise, and achievable within the time frame allocated.

The requirements are loosely grouped by their Information Assurance category. The Information Assurance categories are defined in DoD Directive (DODD) 8500.1. The Information Assurance categories are similar to the Information Assurance services described in the "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment," which was developed before UCR 2008, with one exception. The one exception is that unlike the "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment," DODD 8500.1 does not have a separate category for authorization and includes the functions associated with authorization and access control in the authentication category. The "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment" is a reference document for the UCR and provides an Information Assurance analysis of the protocols, traceability of the DoD Information Assurance requirements, and a threat analysis of the VVoIP design. This document does not provide that background information and instead focuses on the requirements with an overview of the threats.

Table 5.4.2-1, Mapping of Security Services to Security Categories and Goals, shows a mapping of the security services in the "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment," and the security categories in DODD 8500.1. For completeness, the table also maps the security services to the ETSI Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Protocols Framework Definition; Methods and Protocols for Security; Part 1: Threat Analysis, which provides a basis for the threat analysis used in this section and is discussed later.

Table 5.4.2-1. Mapping of Security Services to Security Categories and Goals

"ANALYSIS OF IA REQUIREMENTS AND THREATS FOR THE DoD VVoIP ENVIRONMENT" SECURITY SERVICES	DODD 8500.1 CATEGORIES	ETSI TS 102 165-1 GOALS
Authorization	Authentication (Includes Authorization and Access Control)	Accountability (Includes Non-Repudiation)
Authentication		
Non-Repudiation	Non-Repudiation	
Confidentiality	Confidentiality	Confidentiality
Integrity	Integrity	Integrity
Availability	Availability	Availability

This section concludes with a discussion of the threats and the extent to which they have been mitigated by enforcing the requirements and implementing the CMs. In addition, a brief discussion of the outstanding Information Assurance design issues is discussed. This section is a companion document to the STIGs, which are produced by the DISA Field Security Operations (FSO), and the intent is for this section to complement the STIGs. For instance, the UCR ~~2008~~ specifies the Information Assurance requirements that a VVoIP product must meet to be sold to DoD users. The STIGs specify the configurations that a DoD user must implement to ensure that the system is deployed in a secure manner.

5.4.3 Non-Mitigated Risks

The threat matrix used by the DISN IP VVoIP is based on the one developed by the ETSI TS 165-1. Where necessary it has been modified to reflect the threats that are unique to the DoD environment due to the issues raised in "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment," which also provides a complete discussion of the threats associated with each protocol. The threat matrix was developed to permit a prioritization of the risks associated with those threats in order to target the most urgent threats. It was developed with the knowledge that it is impossible to prevent all attacks, but it is possible to limit the avenues of attack and to react to an attack in an expeditious manner.

The threats identified by the ETSI TIPHON work are focused on the nonphysical threats and do not address the physical threats to the system or all the threats that might arise from the interaction with ancillary equipment (i.e., equipment external to the system such as an external DHCP server).

The TIPHON Threats are extracted from ETSI TS 101 165-1 and additional detail is provided in the following paragraphs. These threats are summarized in Table 5.4.3-1, TIPHON Threats. The "Xs" in Table 5.4.3-1 indicate that the threat impacts the Information Assurance goal and must be mitigated to achieve that goal.

Masquerading or spoofing is the act of pretending to be someone you are not. This threat is often used to get information, deny a service, pervert a service, or misdirect a call. As shown in Table 5.4.3-1, TIPHON Threats, masquerading is a system threat to confidentiality, integrity, accountability, and availability. It is also used as a means to introduce other threats to the system, such as unauthorized access or forgery, eavesdropping, and denial of service.

Table 5.4.3-1. TIPHON Threats

THREAT	GOALS			
	CONFIDENTIALITY	INTEGRITY	ACCOUNTABILITY	AVAILABILITY
Masquerade	X	X	X	X
Unauthorized Access	X (within a system)	X (within a system)	X	X
Eavesdropping	X (on the line)			
Loss or corruption of information		X (on the line)	X	X
Repudiation			X	
Forgery		X	X	
Denial of Service				X

NOTE: The Xs indicate that the threat impacts the Information Assurance goal and must be mitigated to achieve that goal.

Unauthorized access is the act of someone accessing data or services in violation of the security policy. The threat with unauthorized access is that an attacker may access personal or classified information in a database or may be able to make precedence calls causing unnecessary network preemptions. As shown in Table 5.4.3-1, TIPHON Threats, unauthorized access is a threat to both confidentiality and integrity if the action is from within a system. In addition, it is a threat to accountability and availability regardless of where the attacker is located. The principal resultant threats associated with unauthorized access are denial of service, masquerading as a real user, and eavesdropping on other users.

Eavesdropping is a breach of confidentiality caused by the unauthorized monitoring of a communication. It is typically associated with the monitoring of a phone call. Eavesdropping is often used to determine call patterns, gain knowledge of personal information, and to acquire the information necessary to masquerade as another authorized user.

Loss or corruption of data is an attack that compromises the integrity of data. Typically, it involves unauthorized deletion, insertion, modification, reordering, replay, or delay. The goals that are impacted by loss or corruption of data are integrity, accountability, and availability. The loss or corruption of data on a call will affect the integrity of the call and may make the call unintelligible. If the call detail records are destroyed, the accountability for the call will be impacted. Finally, if the loss or corruption of data is significant enough, it could result in a denial of service, which would impact the availability of the system.

Repudiation is when a user involved in a session subsequently denies that the session took place. Non-repudiation is required by the DISN to prevent subscription fraud and to determine responsibility for network management actions. The security service associated with this threat is accountability. In the DoD environment, this threat is not as significant as some of the other threats, but is still a concern.

Forgery is the act of fabricating information and then claiming that the information was received from or sent to another caller. The security goals impacted by this threat are integrity and accountability. One possible scenario for forgery is that an attacker may pretend to be a subscriber and receive calls intended for a legitimate subscriber with no intent to alert the caller, although they may falsely acknowledge that the request was completed. A different situation would involve a subscriber pretending to be the forged subscriber for issuing orders that may negatively impact the operational capabilities of the call recipient.

The final threat is a denial of service attack, which is typically associated with an attacker causing enough congestion on the network that a subscriber's calls cannot be completed or are degraded. In the converged networks planned for the DoD, this may involve either data or VVoIP type attacks. Of particular concern is a VVoIP attack that involves a high number of illegitimate above ROUTINE precedence calls preventing access to the network for legitimate above ROUTINE precedence VVoIP calls. A denial of service attack can occur at all three layers: signaling, bearer, or network management. The principal security goal affected by this type of attack is availability and this vulnerability is more likely to occur in a converged network.

The next step after identifying the threats is to perform a risk analysis of the threats. The method used in the ETSI TIPHON risk model is to score each threat in terms of its likelihood of occurrence and its potential impact. The Threat Risk Score is the product of the likelihood of occurrence and the impact scores. Table 5.4.3-2, ETSI TIPHON Threat Likelihood Scoring

Criteria, and Table 5.4.3-3, ETSI TIPHON Threat Impact Scoring Criteria, are extracted from ETSI TS 102 165-1 and designate the scores that should be used for assessing the system risks.

Table 5.4.3-2 describes the scores that should be used for the likelihood of a particular threat.

Table 5.4.3-2. ETSI TIPHON Threat Likelihood Scoring Criteria

SCORE	LIKELIHOOD	DESCRIPTION
1	Unlikely	According to up-to-date knowledge, a possible attacker needs to solve strong technical difficulties to start the threat, or the motivation for an attacker is very low.
2	Possible	The technical requirements necessary to state this threat are not too high and seem to be solvable without big effort; furthermore, there must be a reasonable motivation for an attacker to perform the threat.
3	Likely	There are no sufficient mechanisms installed to counteract this threat, and the motivation for an attacker is quite high.

Table 5.4.3-3, describes the scores that should be used for the impact of a particular threat.

Table 5.4.3-3. ETSI TIPHON Threat Impact Scoring Criteria

SCORE	IMPACT	DESCRIPTION
1	Low	The concerned party is not harmed very strongly; the possible damage is low.
2	Medium	The threat addresses the interests of providers and subscribers, and cannot be neglected.
3	High	A basis of business is threatened and severe damage might occur in this context.

Following the ETSI TIPHON model, the risk associated with each threat is divided into three categories and all risks scoring a six or nine require CMs. Although risks scoring four do not require CMs, they are still considered major risks and should be mitigated. It should be noted that the risk cannot score five, seven, or eight due to basic mathematics. Figure 5.4.3-1, ETSI TIPHON Threat Risk Score, shows the result of likelihood and impact scores on the overall risk score.

The UC Information Assurance team developed the initial scores and vetted the scores with the user community and industry. The scores are an average based on the feedback since every vendor's Information Assurance solution and every user's implementation is different.

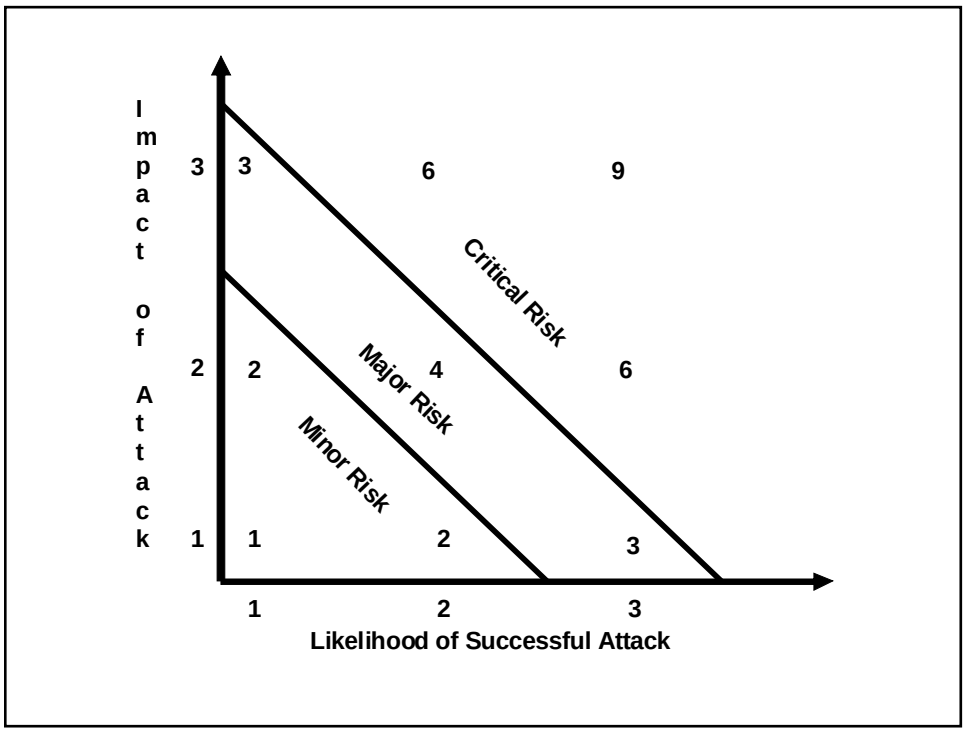

Figure 5.4.3-1. ETSI TIPHON Threat Risk Score

Tables 5.4.3-4 through 5.4.3-12 are extracted from the "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment," and summarize the risk assessments associated with the threats.

Table 5.4.3-4. General Threat Risk Assessment

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G1	Eavesdropping on VVoIP subscriber transport data	2	2	4	Although the SBU voice service is a distinct network from the PSTN, most attacks do occur from inside the network. However, the impact is reduced due to the use of STU/STEs for classified conversations and the use of encryption for all calls.
G2	Corruption of transport data	2	3	6	A user who can eavesdrop on the transport data can manipulate the data stream to issue false orders or to make the communication unintelligible.
G3	Eavesdropping on a valid telephone number to determine its location or to masquerade	2	3	6	Encrypting all layers of the communication should reduce the likelihood. The ability to masquerade the telephone number makes the impact higher.

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G4	Eavesdropping on the signaling data	2	3	6	SIP increases the likelihood of this attack. The information gained in this attack can be used to derive information for other attacks (e.g., a call teardown denial of service (DoS) attack). Call pattern tracking also allows for traffic analysis, which is an operations security (OPSEC) concern.
G5	Corruption of signaling data via malformed packets or protocol fuzzing	2	3	6	SIP increases the likelihood of this occurrence. The modification of the signaling data could be used to derive other types of attacks or for a DoS attack. Malformed messages are protocol messages with incorrect syntax; protocol fuzzing includes malicious messages with proper syntax. Protocol fuzzing interferes with message sequence, confusing the state machine. Unexpected protocol messages can also cause infinite loop parsing and system crashes, along with buffer overflows [G22].
G6	Eavesdropping on network management traffic	2	1	2	The large number of tools available on the Internet makes this task easier, but the impact is minimal.
G7	Corruption of network management data	3	3	9	The closed loop approach to signaling involving the routers would make the impact of this attack high to the voice or video.
G8	Obtaining telephone number from VVoIP end instrument	3	2	6	This information could be used to discern the origination of calls, which can be used by enemies as intelligence.
G9	Denial of service	3	3	9	This is particularly important to voice or video due to the need for assured service for precedence calls. Examples include G11, G12, G21, G22, G23, and G30.
G10	Unauthorized access to data	1	3	3	The primary concern is unauthorized access to CDR. Nevertheless, the security in-depth approach employed minimizes the likelihood of this occurring.

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G11	Flooding the network	3	3	9	This item addresses flooding the network, which is an issue before, during and after call setup. This is a type of DoS attack [G9]. See also valid/invalid registration flooding, valid/invalid call request flooding [G21].
G12	Stolen terminals	3	3	9	In wartime and peacetime scenarios, it is likely that a terminal may be acquired by an enemy agent.
G13	Subscription and toll fraud	3	1	3	Since the DoD is a military organization, this is not as critical since the profit is not the only factor in the solution. This does not mean that it is not important as relates to PSTN charges.
G14	Unauthorized access to network management or subscriber database	2	3	6	The prevention of the dissemination of the locations and sizes of units is critical to the safety of our forces.
G15	Unauthorized access to data in end instruments	2	1	2	The end instruments in the voice or video have limited usable data stored in them. If the end instrument stores private keys, then a possible threat is unauthorized access to the private key and additional related threats become possible.
G16	Masquerading as one legitimate subscriber or signaling device to another	3	3	9	In wartime and peacetime scenarios, it is likely that an enemy agent who gains access to the network will masquerade as a legitimate subscriber.
G17	Man-in-the-middle attack	3	3	9	Although this is an internal threat, the numerous shareware tools available to execute this attack make it likely and the impact is high due to the ability to redirect voice traffic and get access to user data.
G18	Repudiation of actions	2	2	4	The threat depends on the action taken and ability of the system to detect the action rapidly.

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G19	Replay attack	1	2	2	This type of attack could be associated with command related actions, such as "launch all aircraft." These attacks apply to NM, signaling, and bearer streams.
G20	SIP Parser attack	2	2	4	This attack could occur if an unauthenticated EI or SIP signaling appliance was allowed to connect to the network. Another avenue would include the manipulation of the SIP application to create a poorly organized SIP message that is difficult to parse.
G21	SIP Registration or INVITE Flooding – DoS attack	3	3	9	Attacks include valid/invalid registration flooding, and valid/invalid call request flooding. This attack could occur if an unauthenticated EI or SIP signaling appliance was allowed to connect to the network. Another avenue would include the manipulation of the SIP application to generate repetitive registration or INVITEs.
G22	Buffer overflow attack	1	3	3	The likelihood of this attack is small due to the requirement to mutually authenticate all signaling appliances. This attack is associated with malformed SIP messages causing the buffer to overflow.
G23	SIP INVITE	2	1	2	The SIP timers should clear this issue within approximately 32 seconds. In addition, this attack would only affect one phone at a time.
G24	SPAM over Internet Telephony (SPIT)	1	2	2	This attack would have to originate within the SBU voice due to the TDM constraint to the PSTN.
G25	Worms, Viruses, and Trojans	1	3	3	Remove applications that are not VVoIP related from VVoIP appliances. Install antivirus software on appliances that have applications.

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G26	Exploitation of a "zero-day" vulnerability	3	3	9	System remains exposed until an approved fix is available. Close coordination with trusted vendors is needed, along with the ability to rapidly approve/implement fixes once available. Must address any CM, security approval, implementation issues for expeditious turnaround.
G27	Disabling of security controls by authorized users	2	3	6	Various motivations (e.g., avoid complexity, concerns over agency monitoring) prompt authorized users to attempt turning off security mechanisms. Product features to prevent, detect, and/or respond to such circumvention should be included, along with having these features validated (APL).
G28	Exploitation of numerous vendor-specific VVoIP product vulnerabilities	3	3	9	The variety of products that comprise the DISN IP VVoIP introduces the potential for numerous vulnerabilities for exploitation by human threat sources. Although approved products are used, the components must be properly configured and patched on an ongoing basis.
G29	Exploitation of underlying (i.e., not VVoIP-specific) network and/or system vulnerabilities	3	3	9	This item is intended to address all threats considered "general" in the sense of DoD Instruction 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP): "All DoD ISs shall be implemented using the baseline DoD IA controls in accordance with DoD Instruction 8500.2. The baseline DoD IA controls may be augmented if required to address localized threats or vulnerabilities (Section 4.5)." Integration and compliance with the DODI 8500.2 baseline controls will largely mitigate this risk.

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G30	Unintentional flooding	2	3	6	Unintended flooding due to simultaneous end point registration after a power outage, misconfigured end points (e.g., IP phones with too short a registration interval), legitimate flooding (e.g., following a disaster), or end point hardware, software, or firmware malfunctions that cause flooding.
G31	Security devices collectively impact QoS.	2	2	4	Security defense-in-depth depends upon layers of safeguards, including technical components that have the potential to introduce delay (firewalls/NAT, IDS), packet loss and jitter (encryption solutions)—all challenges to VVoIP. Security requirements must be carefully balanced against performance needs.
G32	Components within the system from untrusted sources that could serve as future attack points, such as back doors, logic bombs, etc.	2	3	6	Example: usage of untrusted foreign actor-developed/supplied components, subassemblies, or software embedded within VVoIP, IA, and IA-enabled products.

Table 5.4.3-5. Data Deletion Threat Risk Assessment

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
D1	Eavesdropping of old address	3	1	3	To find the physical location of a user, an enemy may try to eavesdrop on an old address to determine where the terminal was. The likelihood is high due to the mobile nature of DoD subscribers. The risk is reduced by using non-global addressing.
D2	Masquerading as a subscriber to delete data	2	3	6	Once enemy agents gain access to the network they may, in addition to calling people, attempt to access the signaling data to disrupt the ability to place calls. However, the likelihood of this action is less than calling another subscriber.

Table 5.4.3-6. Subscriber Registration Threat Risk Assessment

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
SR1	Illegal registration by an attacker masquerading as a voice or video switch/appliance	1	1	1	Due to the use of TDM for the interface to the PSTN and other networks, the likelihood of this attack is minimal. The impact is also minimal since this would likely be detected very rapidly.

Table 5.4.3-7. Subscriber De-Registration Threat Risk Assessment

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
SD1	Illegal de-registration by an attacker masquerading as a voice or video switch/appliance	1	1	1	Due to the use of TDM for the interface to the PSTN and other networks, the likelihood of this attack is minimal. The impact is also minimal since this would likely be detected very rapidly.
SD2	Subscriber does not allow de-registration by manipulating the end instrument	2	1	2	The impact is minimal since the subscriber should be easily isolated using firewalls and other security mechanisms.
SD3	Subscriber does not allow de-registration by manipulating VVoIP server	2	3	6	This can inhibit the ability of the network to disable illegitimate users and is part of a DoS or flooding attack. SIP manipulation is possible using virus infection.

Table 5.4.3-8. Incoming Call Threat Risk Assessment

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
I1	Masquerading by using someone's ID	2	2	4	Since authentication is mandatory, the likelihood is low.
I2	Masquerading by using someone's ID and authentication	1	3	3	The design of the authentication mechanism should be sufficient to minimize the likelihood of an attack. However, if the mechanism is broken, it makes a large segment of the network vulnerable.
I3	Eavesdropping of the communication on the access interface by use of a session key	1	2	2	Session keys have a shorter lifespan than the time it should take to break the key. The key is not sent in the clear, making it difficult to obtain.
I4	Eavesdropping at the start of a communication on the end instrument	2	1	2	This is possible if call setup is performed before the authentication is completed. Call transfers are also vulnerable to this due to the interval between a call transfer and the rekey.
I5	Modification of routing data	1	3	3	The impact is that data may be routed to bogus or enemy networks; legitimate entities may also be excluded. The likelihood is low due to the defense in depth strategy required.
I6	Message alteration: call black holing	1	3	3	Intermediary configured by an attacker to not pass essential protocol messages. This causes delays in call setup, dropped connections, and other errors.

Table 5.4.3-9. Outgoing Call Threat Risk Assessment

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
O1	Masquerading using a subscriber's ID	1	2	2	This attack is associated with outgoing calls and the likelihood is minimized if authentication is required.
O2	Masquerading using a subscriber's ID and authentication	1	3	3	Authentication would be obtained by methods described elsewhere in this UCR ~~2008~~.
O3	Eavesdropping on the access interface by using a session key	1	2	2	Session keys have a shorter lifespan than the time it should take to break the key. The key is not sent in the clear, making it difficult to obtain.
O4	Eavesdropping on the network	1	3	3	The use of encryption for all layers should minimize the likelihood of this event occurring.
O5	Eavesdropping on the start of a communication on the end instrument	2	1	2	This is possible if call setup is performed before the authentication is completed. Call transfers are also vulnerable to this due to the interval between a call transfer and the rekey.
O6	Eavesdropping on the phone number of a called party	2	1	2	This is possible if call setup is performed before the authentication is completed.
O7	Modification of the dialed number	2	3	6	This attack could result in a precedence call being forwarded to the wrong location.
O8	Masquerading using someone's ID	2	1	2	This is accomplished for the purpose of placing a short call before authentication.

Table 5.4.3-10. Emergency and Precedence Call Threat Risk Assessment

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
E1	Misuse of emergency call	3	1	3	An attacker would place a 911 or emergency call without reason to cause chaos during a crisis or attack. This is important if the authentication mechanisms are compromised or are not implemented for emergency calls. Normally, it would be associated with single sessions.
E2	Misuse of precedence calls	3	3	9	An attacker would place a precedence call without reason to a particular phone to deny that phone's access to other calls. This is important if the authentication mechanisms are compromised.
E3	Manipulation of emergency database information	2	3	6	This could cause calls to be improperly sent to emergency numbers thereby tying up the circuits or sending the emergency calls to invalid destinations.
E4	Manipulation of precedence database information	2	3	6	The likelihood of this attack occurring is higher since this is a critical point of attack for an enemy agent.

Table 5.4.3-11. Survivability Threat Risk Assessment

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
S1	A node in the network is destroyed or disabled	3	3	9	This is a situation very likely in the DoD environment.
S2	A device in the network is disabled or destroyed	3	3	9	Many times an attacker will be able to disable one device before the attacker is detected.

Table 5.4.3-12. Risk Summary

RISK LEVEL	NUMBER OF RISKS	RISK SCORE
Critical Risks	27	6,9
Major Risks	16	3,4
Minor Risks	15	1,2
Total	**58**	

As seen in Table 5.4.3-12, Risk Summary, approximately half of the risks are categorized as critical and require CMs. Sixteen risks were categorized as major risks and the risk should be minimized. Although the other risks are minor, they are still risks that require mitigation and will need to be addressed in the Information Assurance design. The Risk Summary Table is repeated at the end of this section, and it shows the mitigated scores based on the full implementation of the VVoIP Information Assurance design.

NOTE: The risk scores are preference scores, which indicate multiple values that are relatively greater or lesser than the other values. These measures are ordinal. A risk with a score of 2 is considered to be a greater risk than a risk with a score of 1; however a risk of 2 is not necessarily twice as great as a risk of 1. With ordinal measures, the magnitude of the difference between 2 and 1 is not known. In tables such as 5.4.3-4, scores are treated like interval data. A likelihood score of 2 is multiplied by an impact score of 2 to produce a product of 4 which is called a risk score. Under certain conditions, ordinal data may be treated as interval data. In general, the nature of the distribution is the primary consideration.

5.4.4 VVoIP Generic Countermeasures

In "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment," a set of threats and requirements for the DoD VVoIP environment, was identified and these threats were summarized in the preceding paragraphs. A complete discussion of the CMs is provided in "DoD RTS Information Assurance CMs." This section describes the process used to develop the CMs required of the DoD VVoIP environments based on those threats and requirements and summarizes the generic CMs developed to mitigate the threats. The first step in the process is to develop an initial set of recommended CMs that tentatively mitigate the threat to an acceptable level.

5.4.4.1 Recommended Countermeasures

The recommended CMs were developed using an iterative process involving the vendor and DoD communities to mitigate the threats associated with a DoD VVoIP environment. The CMs are presented in a generic manner to ensure they do not mandate a technical solution, and are provided as part of the systems engineering process for developing the Information Assurance design. There is no intent to mandate a countermeasure on an appliance or system and they should not be considered requirements. The system design, and its associated requirements, will define the technical solution for the system and its appliances and a specific countermeasure may or may not be used dependent on the design. The threats associated with ancillary services and TDM technologies have not been addressed completely. Therefore, the CMs described below do not address the threats associated with ancillary equipment and TDM technologies completely. Before discussing the CMs, it is important to define the terms used in the discussion.

1. Registrant. An appliance that is used to register with the network to seek and gain authority to invoke services or resources from the network. Registrants are typically associated with primary and alternate registrars. Examples of registrants are EIs, AS-SIP End Instruments (AEIs), EOs, PCs, and LSCs.

2. Registrar. The appliance that stores the location of a registrant and its profile. The profile is used to define the services to which a registrant is authorized (or a user via the registrant). In the DoD VVoIP environment, examples of the registrar include LSCs, AEI and DoD PKI servers. A registrar may reside on the same appliance and be integrated with a Service Point of Attachment (SpoA).

3. Service Point of Attachment. An SpoA is an appliance to which a registrant establishes a session over the IP network or TDM network. The session may be established to pass signaling or network management traffic. In the DoD VVoIP environment, examples of an SpoA are LSCs, MFSSs, SSs, directory servers, or gateways.

4. Transport Point of Attachment (TpoA). A TpoA is an appliance that is used to provide transport of a session over a network. Examples of transport appliances in the DoD VVoIP environment include routers, LAN switches, firewalls, EBCs, MFSS, and gateways.

Figure 5.4.4-1, Interaction between VVoIP Information Assurance Components, shows the interactions between the different countermeasure elements.

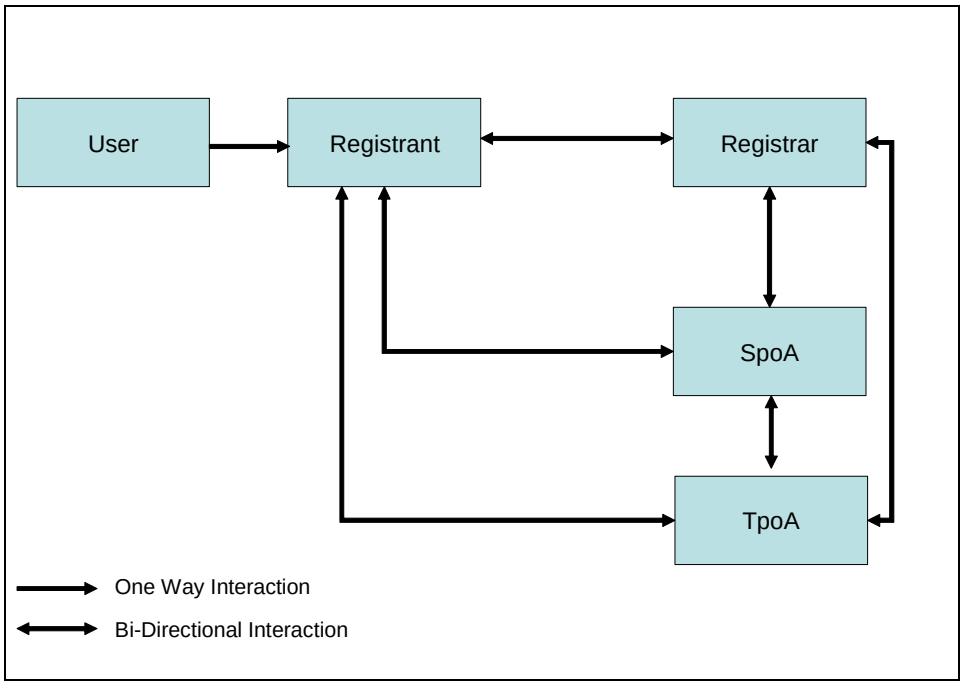

Figure 5.4.4-1. Interaction between VVoIP Information Assurance Components

5.4.4.2 Access Control Countermeasures

1. C1 – Access Control to Services. The system should validate, based on prior authentication, the privileges to which a user has authorization before granting access to services.

2. C2 – Access Control to Database. The system should validate, based on prior authentication, the privileges to which a user has authorization before granting access to a database.

3. C3 – Access Control to Sensitive Information in EI and AEI. The system should validate, based on prior authentication, the privileges to which a user has authorization before granting access to sensitive information stored on an EI or on a AEI.

4. C4 – Access Control to System Software. The system should validate, based on prior authentication, the privileges to which a user has authorization before granting access to the system software. This software includes the software needed to provide VVoIP as well as the operating system software.

5. C5 – Access Control to System Hardware. The system should control access to the use of system hardware from users who are not authenticated.

6. C6 – Access Control to System Resources. The system should protect system resources from users who are not authenticated.

7. C7 – Access Control between Network Resources. The system should protect one network resource from another network resource unless there is a defined requirement for those resources to interact.

5.4.4.3 Authentication Countermeasures

1. A1 – Authentication of the EI and the AEI by the Registrar. The EI and AEI should contain a unique identity that identifies the EI and the AEI to the registrar, and authentication should confirm this identity through proof of knowledge of a secret shared by the registrar and the EI and the AEI, or by the use of a public key cryptosystem. This countermeasure is the corollary of A2.

2. A2 – Authentication of the Registrar by the EI and the AEI. The Registrar should contain a unique identity that identifies the registrar to the EI and the AEI, and authentication should confirm this identity through proof of knowledge of a secret shared by the registrar and the EI and the AEI, or by the use of a public key cryptosystem. This countermeasure is the corollary of A1.

3. A3 – Authentication of the EI and the AEI by the SpoA. Before providing service to the SpoA, the SpoA should authenticate the EI and the AEI. This countermeasure is the corollary of A4.

4. A4 – Authentication of the SpoA by the EI and the AEI. Before transmitting to a SpoA, the EI and the AEI should authenticate the SpoA to ensure that it is the actual SpoA assigned by the registrar. This countermeasure is the corollary of A3.

5. A5 – Authentication of the SpoA by the Registrar. The registrar should authenticate the SpoA before directing an EI and AEI to use that SpoA. This authentication should be based upon a secret shared by the registrar and the SpoA. This countermeasure is the corollary of A6.

6. A6 – Authentication of the Registrar by the SpoA. The SpoA should authenticate the registrar requesting service before granting that service. The authentication should be based upon a secret shared by the registrar and the SpoA. This countermeasure is a corollary to A5.

7. A7 – Authentication of the User to the Appliance. The user should authenticate to the appliance to protect against misuse. This countermeasure does not have a corollary.

8. A8 – Authentication of the SpoA by the TpoA. Before transmitting to a SpoA, the TpoA should authenticate the SpoA to ensure that it is the actual SpoA to which it is assigned. This countermeasure is the corollary of A9.

9. A9 – Authentication of the TpoA by the SpoA. Before transmitting to a TpoA, the SpoA should authenticate the TpoA to ensure that it is the actual TpoA to which it intends to transmit. This countermeasure is the corollary of A8.

10. A10 – Authentication between SpoAs. Before transmitting to a SpoA, the SpoA should authenticate the other SpoA to ensure that it is the actual SpoA to which intends to transmit. This countermeasure does not have a corollary.

11. A11 – Authentication between TpoAs. Before transmitting to a TpoA, the TpoA should authenticate the other TpoA to ensure that it is the actual TpoA to which intends to transmit. This countermeasure does not have a corollary.

5.4.4.4 Non-Repudiation Countermeasures

N1 – Non-Repudiation of User Modifications to Appliance Resources. The appliances should ensure that non-repudiation is associated with any modifications made to an appliance's resources to include the operating system, files, applications, or databases.

5.4.4.5 Data Confidentiality Countermeasures

1. E1 – Confidentiality of User Communication on the EI and the AEI. The system should provide confidentiality for bearer stream at the EI and the AEI for originating and terminating sessions.

2. E2 – Confidentiality of Signaling on the EI and the AEI. The system should provide confidentiality for the signaling stream at the EI and the AEI for all originating and terminating sessions.

3. E3 – Confidentiality of Signaling between SpoAs. The system should provide confidentiality for the signaling between SpoAs. Signaling may include session keys, call-forwarding numbers, network management traffic, and personal data.

4. E4 – Confidentiality of Signaling between SpoA and TpoA. The system should provide confidentiality for sessions between the SpoA and the TpoA. The signaling may consist of signaling or network management traffic. This may be accomplished using physical protection or cryptographic protections.

5. E5 – Confidentiality of Communication between TpoAs. The system should provide confidentiality for sessions between TpoAs. The communication between TpoAs may consist of signaling or network management traffic. This may be accomplished using physical protection or cryptographic protections.

6. E6 – Confidentiality of Communication between SpoA and Registrar. The system should provide confidentiality for sessions between SpoAs and registrars. The communication may consist of signaling or network management traffic. This may be accomplished using physical protection or cryptographic protections.

7. E7 – Confidentiality between User and Appliance. The system should provide confidentiality for sessions between an authenticated and authorized user and an appliance for network management purposes.

8. E8 – Confidentiality of Data at Rest. The system should provide confidentiality for data at rest. The data may be stored in a file or a database.

9. E9 – Confidentiality between the Registrar and the Registrant. The system should provide confidentiality for registration and de-registration of appliances to the network.

5.4.4.6 Data Integrity Countermeasures

1. I1 – Signaling Integrity. The system should ensure integrity for signaling messages. Types of signaling messages include SIP, H.323, and routing updates.

2. I2 – Bulk Data Transfer Data Integrity. The system should ensure integrity for bulk data transfers. Bulk data transfers include call detail records (CDRs).

3. I3 – Appliance Data Integrity. The system should ensure the integrity of data written, read, or stored on an appliance.

4. I4 – Appliance System Integrity. The system should ensure the integrity of the operating system and the applications on the appliance. This shall include unauthorized operating system or application modifications.

5. I5 – End Instrument Transport Integrity. The system should ensure the integrity of the bearer packets transmitted between the end instruments.

5.4.4.7 Survivability/Availability Countermeasures

1. S1 – Diversity of Network Connections. The system should ensure high availability using diverse geographical distinct connections for designated locations throughout the network. In addition, the connections should be diverse from both physical and logical perspectives. Sites that require diverse geographic distinct connections are typically C2 sites. However, non-C2 sites sometimes require diverse connectivity dependent on the mission and network topology.

2. S2 – Redundancy of Hardware and Software. The system should have sufficient redundancy in hardware and software to ensure that the required availability is achievable based on the computed failure rates for the hardware and software.

3. S3 – Out-of-Band Network Management Capability. The system should have an out-of-band network management capability for use during network outages or for when network resources are not reachable during Information Assurance attacks.

4. S4 – System Power Redundancy. The system should have sufficient backup power for use during power failures based on its usage and user requirements.

5.4.4.8 Miscellaneous Countermeasures

Some CMs overlap many assurance categories and they are classified as miscellaneous CMs. Each of the assurance categories are subject to newly-discovered ("zero-day") vulnerabilities.

Miscellaneous CMs contribute to a layered, defense-in-depth architecture for zero-day addressing and other vulnerabilities.

Product Assurance: VVoIP components should be purchased from reputable vendors that, at a minimum, conduct internal pre-release reviews and provide vulnerability fix support for their products. Details of these provisions should be documented as part of the vendor warranty to the Government that addresses product defects.

5.4.4.9 Privacy Countermeasures

1. P1 – Physical Security. The system infrastructure should be placed in a secure facility that only permits access by authenticated and authorized personnel.

2. P2 – Personal Data Security. Personally Identifiable Information (PII), especially Social Security numbers, in the system infrastructure should be minimized to the maximum extent possible. Where present, the PII should be protected in accordance with DoD information assurance and privacy policy and guidelines.

5.4.4.10 Network Management Countermeasures

M1 – Threshold Exception Management System Notification. The system should notify a designated network management system when predefined thresholds are exceeded. A threshold may consist of a single event (e.g., an audit log failure) or multiple events (e.g., multiple failed login attempts).

After developing the CMs, the next step in the Information Assurance Process was to develop a VVoIP Information Assurance design that implements these CMs. Based on that, design a set of requirements was derived. An iterative process was used due to the many interdependencies involved.

5.4.5 ~~VVoIP~~ Information Assurance Design

5.4.5.1 ~~VVoIP Component~~ Physical Security

Physical security for ~~a VVoIP~~ systems specified in this UCR are~~is~~ the responsibility of the installing B/P/C/S. There are essentially two sets of requirements associated with a complete ~~VVoIP~~ UC system. The EIs have one set of physical security requirements while the network (LAN switches and routers), ~~and~~ signaling products (i.e., LSC, MFSS, SS, MG, etc.), and Security Devices require another set of requirements. A full definition of physical security requirements is beyond the scope of this section of the UCR.

~~The EIs of a VVoIP product are located in many different types of facilities. Their physical security is dependent upon the physical security afforded by the facility in which they are housed. The physical security of the facility is dependent upon the sensitivity and/or classification of the information that it contains or processes.~~

The physical security for the ~~VVoIP~~ UC product network infrastructure and signaling appliances must limit physical access to all the associated appliances and cable terminations. Sensitivity and/or classification of the product have no bearing on this requirement. This means that the supporting infrastructure for the total product must reside, minimally, behind locked doors. This may, however, be minimally provided by a lock on a cabinet housing a LAN switch in the open (i.e., an unsecured area). ~~Again, as w~~With the EI and the AEIs, this is typically afforded by the facility in which the equipment/infrastructure is housed (e.g., locks and/or access control on doors of rooms and closets housing the equipment).

Facility security requirements fall under the purview of "DoD Traditional Security." ~~These requirements are well beyond the scope of the UCR.~~ A subset of these requirements is provided in the VVoIP STIG and other related DISA STIGs.

Vendors must support their customer's need to comply with the DoD system physical security requirements for ~~VVoIP~~ UC products. This support is to be provided in the form of locking kits for any equipment that the vendor normally provides in a cabinet. If a cabinet lock is not provided normally in the vendor's commercial offering, optional locking kits must be made available that work well with the vendor's cabinet. All cabinet locking mechanisms must be robust enough to resist prying the cabinet open.

5.4.5.2 ~~VVoIP Appliance~~ Security Design

The ~~VVoIP~~ UC product security design uses a defense in-depth approach that is based on best commercial practices. The product security defenses are categorized as follows and discussed in the following paragraphs:

- User Roles
- Hardened Operating Systems
- Auditing
- Application Security
- Redundant Systems

Additional defenses may be added dependent on the specific threats associated with a product.

5.4.5.2.1 User Roles

In general, t~~T~~here are three types of users related to a ~~VVoIP~~ UC product, which are segmented into two different categories: users of the system services and administrative users of the product. This becomes confusing due to the unqualified and repeated use of the word "user." One must be aware of and remember what area of the product is being discussed (i.e., its services or its administration, configuration, or maintenance) in order to be sure of the context of the word.

Essentially, a user of product services has one role. He or she uses the services that the product provides and they are referred to in this UCR section as application users. Such a user may be a "privileged application user" who has permission to use certain restricted services, such as the ability to initiate a FLASH precedence session. Such a user may be required to authenticate to the product in some fashion (such as entering a personal identification number (PIN) code to identify the user (called User ID) and a different PIN (called password) to authenticate the user) in order to receive access to their "privileged" service. There may be multiple levels of privileged service, which might be considered "service user roles" by some readers.

Administrative users are those users that are tasked with the configuration, operation, or maintenance of the system. These users are usually referred to as system administrators. System administrators fulfill different roles based on their duties, responsibilities, or job description/function. DoD policy requires that system administrators receive only those system privileges or access to commands that are required to perform their duties (i.e., role-based access). System administrators who are limited to selected applications on the system are designated application administrators.

System administrators receive their privileges or access to commands based upon Discretionary Access Control (DAC), which provides authorization control. Discretionary Access Control is a role-based feature that grants a system administrator specific permission to perform various functions when accessing the product. Such permissions are established in accordance with the job functions and responsibilities (role) of the individual. Permissions are established by the responsible security officer (i.e., the Information Assurance Officer (IAO) or system security administrator), and stored in the system memory or its configuration files. The security officer also establishes the relationship in the system between authorized command class(es) or group(s).

Products that are developed with various levels of authorization or command access must support DAC requirements. This can be achieved by user privileges or group privileges. The methods to access resources may vary depending on hardware and software products.

Examples of system administration roles are as follows:

1. Tier 3 Engineer (Troubleshooter – Initial Support). This role may only have privileges and access to commands that allow him/her to view operational statistics, alarms, and some specific level of appliance or system configuration. This role may not have the ability to change any configuration settings. This could be considered Tier 3 support.

2. Tier 2 Engineer. This role would have all the capabilities of the troubleshooter role with the added privileges and access to certain commands that allow him or her to make some but not all configuration changes.

3. Tier 1 Engineer. This role would have privileges and access to all commands for troubleshooting and system configuration.

4. Provisioner/Administrator. This role may only have privileges and access to commands that allow him/her to provision circuits, configure end instruments and/or features. This role may have the ability to troubleshoot some aspects of the system.

Another scenario is the case of a database administrator or application administrator role that only has rights to access the database or an application that they manage but does not have rights to access the administration of the operating system on the platform that support one or more databases or applications.

Similar roles or levels of privilege and DAC to those described above are required for DoD information systems. These equate to the normal system administrator roles. The granularity of DAC provided is dependent on the capabilities of the specific system being managed.

The third type of user required for DoD systems is the Auditor, which is short for Security Auditor. This role has none of the normal system administrator privileges or access. The normal system administrator role does not have access to auditor level commands. The auditor role only has access to commands related to the security or audit logs, and is associated with the system security administrator.

5.4.5.2.2 Hardened Operating Systems

Multipurpose or general-use operating systems are delivered with none, or a minimal number, of security features enabled. Access to critical areas of the operating system as well as application and data files is sometimes unrestricted. Additionally, some of these operating systems are delivered with inherent security vulnerabilities, both known and undiscovered. The process of "hardening" an operating system is the process of restricting access to those system areas and functions that could be detrimental to the security of the system and mitigating the known and/or discovered security vulnerabilities. The implementation guidelines associated with common operating systems are found in the STIGs developed for the operating system and are different for every operating system.

5.4.5.2.3 Auditing

In this UCR section, auditing refers to the logging and analysis of security related events. Auditing and recording the events occurring to or within an appliance of the APL product is critical to maintaining accountability. This is accomplished by tracking security and configuration related changes, which provides the system security administrator or Information Assurance manager vital information to reconstruct what may have occurred before a system crash or other situation. Security auditing is necessary for the reconstruction of system events that have led to a security incident in support of disciplinary action or prosecution. This information may also allow the system manager to restore a system to its correct configuration and to determine the cause of the problem. The term "history file" may or may not relate only to security. Some systems such as telecommunications appliances record every transaction performed by the appliance. History files may or may not contain auditable security events. A determination must be made for each appliance regarding the location of the security audits. Appropriate security record events must be captured, recorded, retrieved, protected, reviewed, and archived on a regular basis.

The DODI 8500.2 is the primary driver of auditing requirements. The DODI 8500.2 IA control Enclave and Computing Environment Audit Trail Protection-1 (ECTP-1) states:

> "The contents of audit trails are protected against unauthorized access, modification or deletion."

DoD requirements also state that all system and network devices perform security auditing and that auditing records are placed in an unalterable audit or history file that is available only to those individuals authorized to analyze system or network appliance access and configuration activity. This implies that the audit log must be separate from any other system logs.
The DODI 8500.2 states the following regarding audit record content:

Audit records include:

Enclave and Computing Environment Audit Record Content-1 (ECAR-1); Base level for information sensitivity = public

- User ID
- Successful and unsuccessful attempts to access security files
- Date and time of the event
- Type of event

Enclave and Computing Environment Audit Record Content2 (ECAR-2); Adds items for information sensitivity = sensitive

- Success or failure of event
- Successful and unsuccessful logons
- Denial of access resulting from excessive number of logon attempts
- Blocking or blacklisting a user ID, terminal or access port, and the reason for the action
- Activities that might modify, bypass, or negate safeguards controlled by the system

ECAR-3; Adds items for information sensitivity = classified

- Data required to audit the possible use of covert channel mechanisms
- Privileged activities and other system-level access
- Starting and ending time for access to the system
- Security relevant actions associated with periods processing or the changing of security labels or categories of information

The above DoDI 8500.2 requirements are mapped, interpreted, and augmented with best practice, as shown below.

At a minimum, the following events are to be audited on the system and network devices:

- Logons and logouts
  - Starting and ending time for access to the system
- Excessive logon attempts/failures
  - Denial of access resulting from excessive number of logon attempts
  - Blocking or blacklisting a user ID, terminal or access port, and the reason for the action

- Remote system access
- Change in privileges or security attributes
  - Activities that might modify, bypass, or negate safeguards controlled by the system
- Change of security levels or categories of information
  - Security relevant actions associated with periods processing or the changing of security labels or categories of information
- Failed attempts to access restricted system privilege levels or data files
- Audit file access
- Password changes (not the passwords)
- Device configuration changes
  - Privileged activities and other system-level access
- Other
  - Data required to audit the possible use of covert channel mechanisms

At a minimum, the following information is recorded in the audit log for each event that is audited:

1. Date and time of the event
2. Origin of the request (e.g., terminal/workstation ID, port ID, IP address, etc.)
3. Unique ID of the user who initiated the event
4. Type of event
5. Success or failure
   a. Success or failure of event
   b. Successful and unsuccessful logons
   c. Successful and unsuccessful attempts to access security files

6. Description of modification to configurations

NOTE: A vendor's system, appliance, or product should support the audit requirements for classified products so that they can be purchased for use in classified systems. There may be additional requirements that it will need to meet.

DoDI 8500.2 also requires that audit logs be:

> "…regularly reviewed for indications of inappropriate or unusual activity" (ECAT-1) on MAC-3 and/or systems processing sensitive and public information.

Additionally, for MAC 1 and 2 and/or systems processing classified information it states:

> ~~,~~"An automated, continuous on-line monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications, and with a user-configurable capability to automatically disable the system if serious IA violations are detected (ECAT-2). These requirements indicate that they are to be reviewed regularly and additionally for classified and/or mission critical systems, auditing should generate alarms to 'immediately alert personnel' of security issues."

The process of auditing security events can generate large volumes of data on busy systems. For this reason, audit logs are to be retrieved or removed from the system on a regular basis. Since audit logs contain information that may be required in support of administrative or prosecutorial actions, they must be protected. In some cases (i.e., Microsoft Windows-based systems), audit log protection is provided by halting the system operation if the audit capability fails.

DoDI 8500.2 ECRG-1 states:

> "Tools are available for the review of audit records and for report generation from audit records."

The tools that are referenced are software tools provided by the vendor that can interpret the vendor's audit log file format to allow offline viewing and analysis of the logs, as well as the generation of reports ~~VVoIP~~ from the data contained therein.

5.4.5.2.4 Application Security

DoD application security requirements are based on and are implemented in accordance with DoD Information Assurance policy requirements. These requirements are detailed in the DoD Application Security Checklist and DoD Application Development STIG. Basic application

security requires that the application must not alter the security posture of the supporting operating system or other applications on the platform. In addition, applications must not change operating system files. Applications may rely on the operating system for some Information Assurance functions or may include some or all Information Assurance enablement features in the application. Applications that provide management capabilities of a system should be Information Assurance enabled. These applications should provide, at a minimum, for identification, authorization, roles/command classes, and auditing in accordance with the documents mentioned previously in this section.

5.4.5.2.5 Redundant Systems

Products that support critical services, such as voice communications or security services, should be designed with enough redundancy to prevent single point of failure issues that could affect more than a threshold number of end points. This is partially driven by the percentage of "uptime" that is targeted for the overall system. Every critical product function should have a backup. This includes power distribution, signaling appliances, other critical servers, core LAN hardware (routers and switches), boundary hardware (EBCs and CE Routers), and data links. A certain level of redundancy is appropriate. The core and distribution segments of a LAN, for example, should be redundant. The uplinks to the access segment switches should be redundant also. Redundancy for access segment switches and the distribution cabling to the end points does not make sense. One design concern is that if the access segment switch supports more than the threshold number of voice end points, which is typically driven by the Telcordia Technologies GR-512-CORE reliability requirements, then it is recommended that the end points be split among different switches. If this cannot be done, the switch should have redundant processors and power supplies.

It is beyond the scope of this section to define every item that needs to be redundant. This determination must be made based on good design criteria and best commercial practices. Nevertheless, ~~UCR,~~ System Quality Factors section in section 5.3 of this UCR specifies many requirements associated with redundancy, and these should be used as a requirement baseline for the systems to which the documents apply.

5.4.5.3 ~~V~~VoIP UC Component Interactions

One of the principal tenets of any Information Assurance design is the separation of components (i.e., traffic, appliances, and users) and/or services from each other based on their characteristics. Still, a converged network requires the opposite in that appliances within a converged network may service the voice, data, and video applications. As a result of this conflict, the interactions between the various component segments must be controlled to ensure that an attacker that gains access to one segment does not gain access to, nor can affect, the other segments. In addition, interaction control between various segments is also used to prevent configuration or user errors in one segment from impacting other segments. The actions of normal users of converged

network services must not affect the other services, more specifically the voice service. The principal mechanisms that are used within this design for segmenting the network are VLANs, segmented IP address space or subnets, and VPNs and are used in combination with filters, access control lists (ACLs), and stateful packet inspection firewalls (VVoIP Stateful Firewalls) to control the flow of traffic between the VLANs and VPNs.

Figure 5.4.5-1, Notional Example of Voice and Data ASLAN Segmentation, presents the simplest type of converged LAN with only voice and data applications. Those readers familiar with the architecture defined in the DISA Enclave STIG will recognize many similarities between Figure 5.4.5-1 and the recommended architecture defined in the Enclave STIG. Separate VLANs are established between voice and data applications and the Layer 3 switches are responsible for providing access control between the different VLANs using filtering techniques, such as ACLs. In this type of deployment, appliances are classified as VVoIP appliances or data appliances and it may be possible to avoid deploying appliances that service both VVoIP and data appliances. At the CE Router, separate VPNs may be established, if necessary, to segment the voice traffic from the data traffic as the packets transit the DISN WAN. In addition, VPNs may be used to extend the local enclave to remote offices of the same organization, telecommuters, and travelers. Also, the VVoIP traffic is routed from the CE Router to the PE Router along the same path as the non-VVoIP traffic. The only connection to the PSTN is through a TDM interface using PRI or CAS signaling so that there is not interaction between the VVoIP system and commercial VVoIP IP networks. Moreover, it is important to note that the LSC has two separate interfaces; one for signaling and bearer traffic and one for network management traffic.

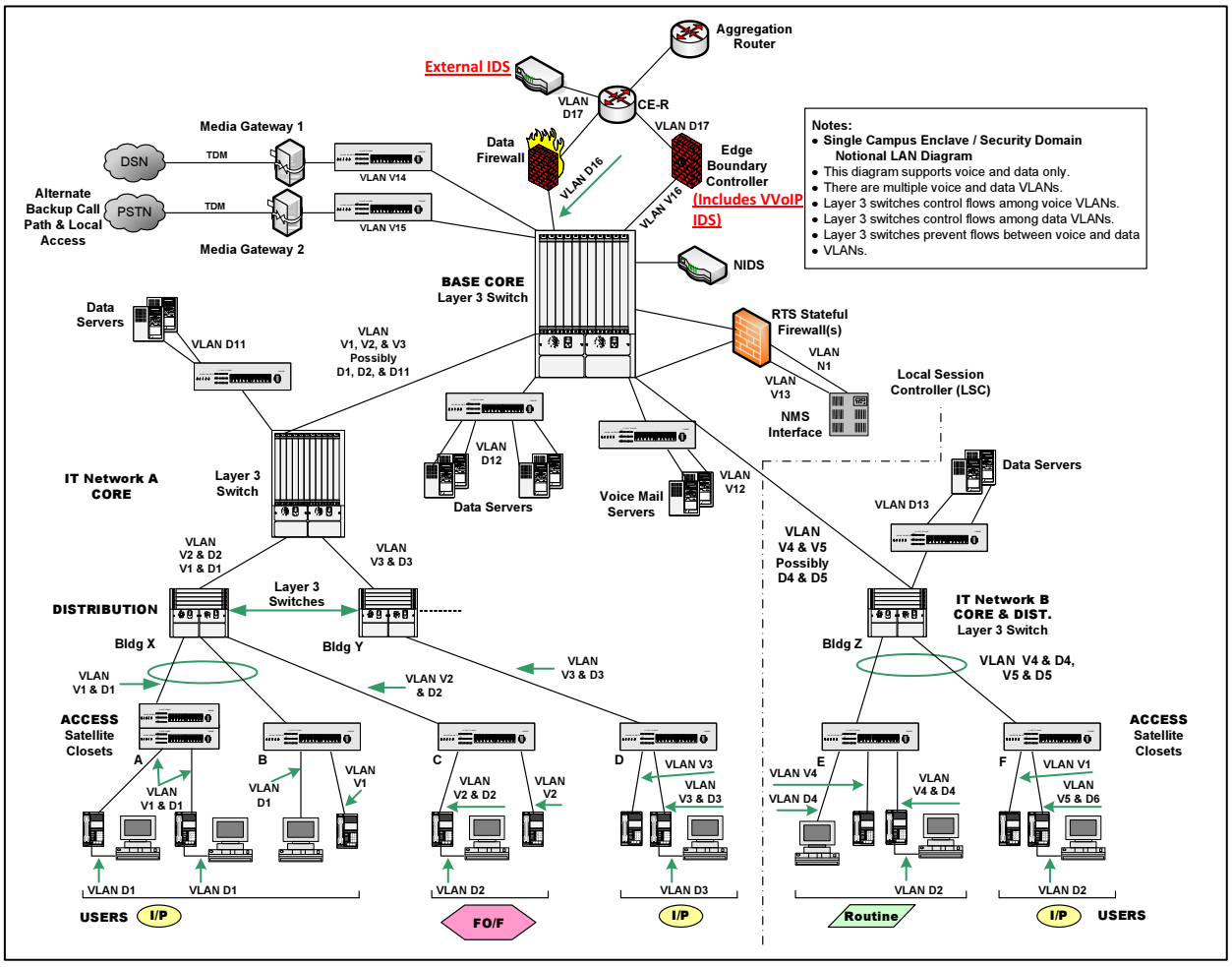

Figure 5.4.5-1. Notional Example of Voice and Data ASLAN Segmentation

The 802.1Q VLAN tagging of the packet for the appropriate VLAN should occur at the appliance, but may occur at the first LAN switch if the appliance is not capable of 802.1Q VLAN tagging. To comply with this, the ASLAN permits port-based and MAC-based VLAN tagging. Although VLANs are an important component of the Information Assurance defense in depth approach used here, the reader should remember it is only one component. If an EI or a AEI supports a subtended data computer/workstation, it must perform several unique functions. The first function is that it should be capable of VLAN tagging the data traffic with a different VLAN tag than the voice traffic. In addition, it must be capable of routing the VVoIP traffic and the data traffic to the appropriate VLAN. The objective of this function is to ensure that the data applications on the workstation do not have visibility to the voice related packets.

A more complex design involves appliances that support multiple types of applications like softphones and videophones. Figure 5.4.5-2, Notional Example of Voice, Video, Softphone, Videophone, and Data ASLAN Segmentation, shows the VLAN segmentation associated with this complex design. To simplify the design, all voice, video, and data sessions associated with a

VTC are VLAN tagged (and DSCP marked) as a video session. In the case of videophones, the videophone may be used for voice or video applications. In this case, the audio and video traffic from the videophone may reside in the voice VLAN(s). The VTC only systems, desktop or room size, should have their own VLAN and addressing structure.

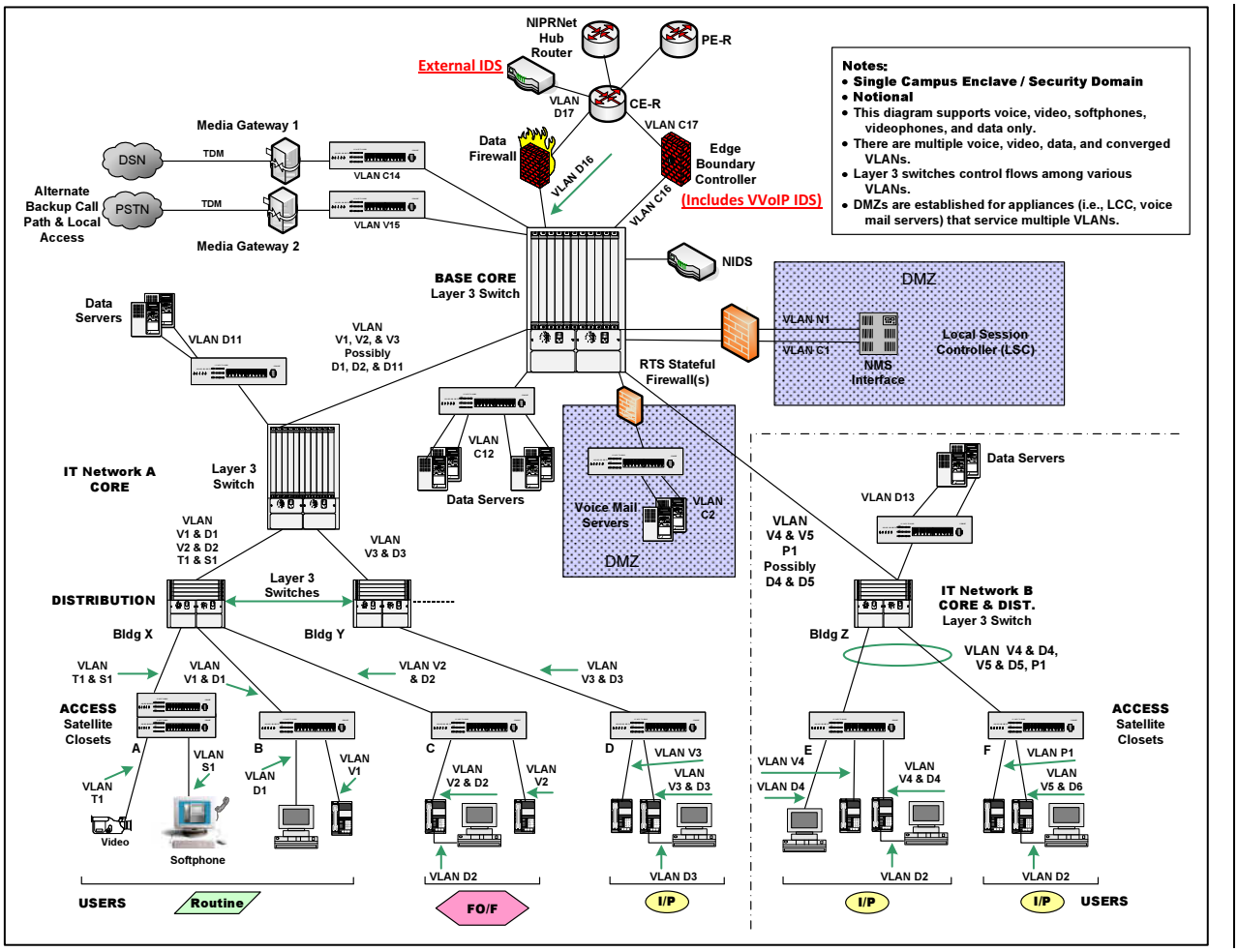

Figure 5.4.5-2. Notional Example of Voice, Video, Softphone, Videophone, and Data ASLAN Segmentation

Demilitarized zones are created for appliances that must service multiple segments of the converged network. An example is the LSC, which must service voice, video, videophone, and softphone appliances. Since access control between the various VLANs is significantly more complex, filtering is not adequate to achieve this goal and VVoIP stateful firewalls are needed to ensure that only authorized packets are able to transit the VLAN boundaries. The stateful firewall may have the complete functionality of an EBC, but this is not required.

In addition, if the softphones are used in remote connectivity situations, such as for a long local for a tactical deployed system, the system must be capable of supporting a VPN for VVoIP

traffic from the PC to the LSC. It is essential that the data and VVoIP traffic must be separated into the appropriate VLAN at the earliest point in the path. In the long local scenario for a tactical user, this separation would likely occur at the Teleport facility.

Finally, an alternative not shown in the diagrams involves an LSC that has separate interfaces for the H.323, AS-SIP, and network management traffic. In this scenario, the ASLAN should have an H.323 VLAN, an AS-SIP VLAN, a data VLAN, and a network management VLAN as a minimum. Each network will typically have unique requirements and topology, and the VLANs implemented will depend on the local network needs.

Each of the following represents a separate VLAN:

1. VoIP EIs and AEIs (multiple VLANs recommended for large sites)*

2. VoIP LSCs, SSs, and configuration servers*

3. Separate VLANs for other voice/VVoIP related servers

    a. Voice mail or unified messaging (voice mail and e-mail)*
    b. Computer Telephony Integration (CTI)
    c. Automatic Attendant/Call Director (ACD)
    d. Call center or operator's systems
    e. Emergency messaging system servers
    f. Multipoint controllers for conferencing: VTC and/or audio only
    g. Streaming video servers (video streams share the data VLANs)

4. Media Gateways*

    a. VoIP EIs that are part of a CTI, ACD, or call center/operator's system

5. VoIP EIs that have an integrated VTC capability

    a. VoIP and VTC video can share the same VLAN
    b. Multiple VLANs recommended for larger sites

6. Stand-alone desktop VTC units

    a. Units associated with and/or controlled by the VoIP LSC can reside in the VoIP EI VLAN(s).

    b. Workstations running softphone applications (DAA Approved)*

c. Workstations running desktop VTC applications (DAA Approved)

7. Collaboration tools: The VTC portion should use the appropriate VVoIP VLAN(s) if technically feasible while the data applications (e.g., whiteboard, file sharing, etc.) must use the data VLAN(s).

NOTE: Items marked with an asterisk (*) are currently required in the VoIP STIG.

Figure 5.4.5-3, Component Interaction Flow Diagram, provides a different depiction of the interactions between various VLANs within a B/P/C/S. The illustrations in this section are notional and address the scenario where ancillary services are internal to the system. The information is only provided as reference material and each B/P/C/S will determine its VLAN needs and boundaries based on its tailored requirements and security profile.

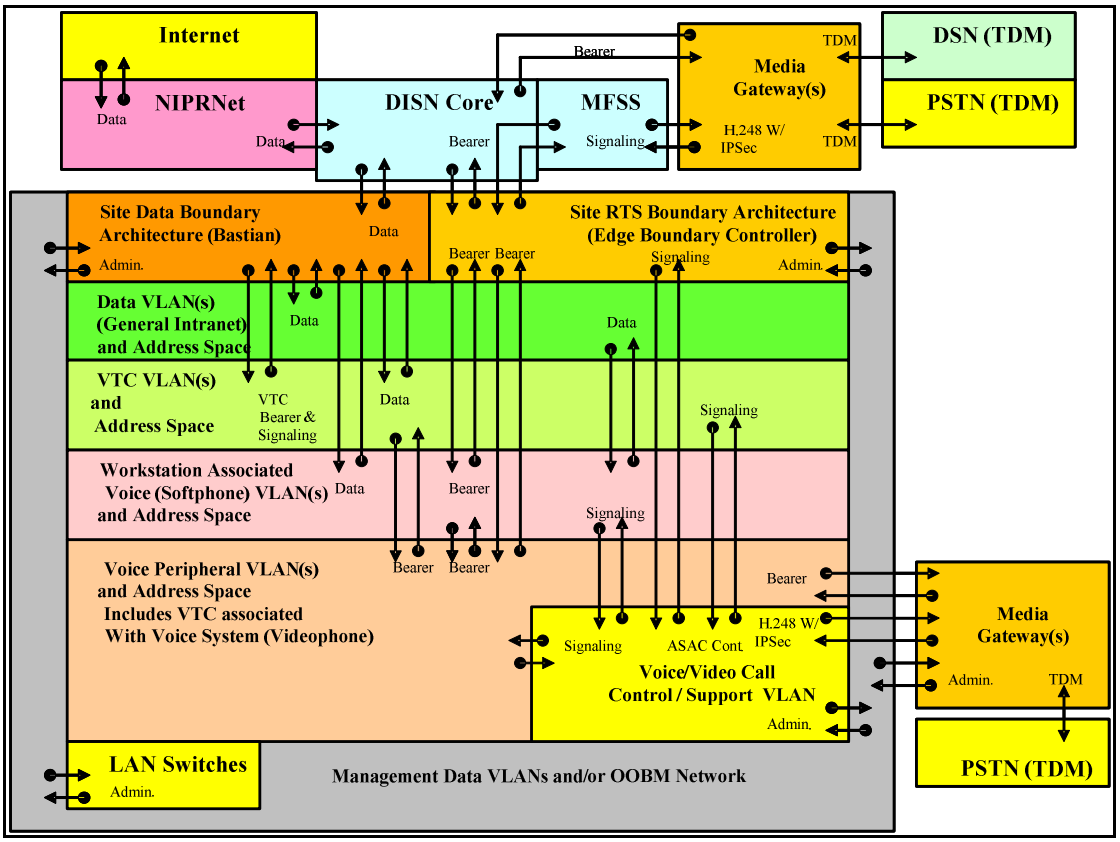

Figure 5.4.5-3. Component Interaction Flow Diagram

5.4.5.4 VVoIP Protocol Design

5.4.5.4.1 Overview

The VVoIP protocol Design consists of a combination of standards based protocols and proprietary based protocols. Within an APL Product the vendor is allowed to implement proprietary protocols for signaling (e.g., between the End Instrument and the LSC or between the LSC and the Media Gateway), but standards-based protocols are required for interfaces to external network management, signaling and transport appliances. Although EIs may use proprietary protocols, AEIs may not. The AEIs are required to use AS-SIP for signaling. Every proprietary protocol must be secured in a manner that is at least as secure as can be achieved using a standardized protocol. For instance, the VVoIP design mandates the use of TLS with AS-SIP to provide confidentiality and integrity. AS-SIP, in combination with TLS, could be used for the signaling between the EI and the LSC, but is not required (AEIs require AS-SIP). Since every proprietary protocol must be secured in a manner that is at least as secure as can be achieved using a standardized protocol, if a vendor chooses to use a proprietary protocol for that interface, it must be as secure as that which can be achieved by using AS-SIP with TLS. Figure 5.4.5-4 presents the different protocols that are allowed in the VVoIP system and discriminates between interfaces that permit proprietary protocols and ones that require standardized protocols.

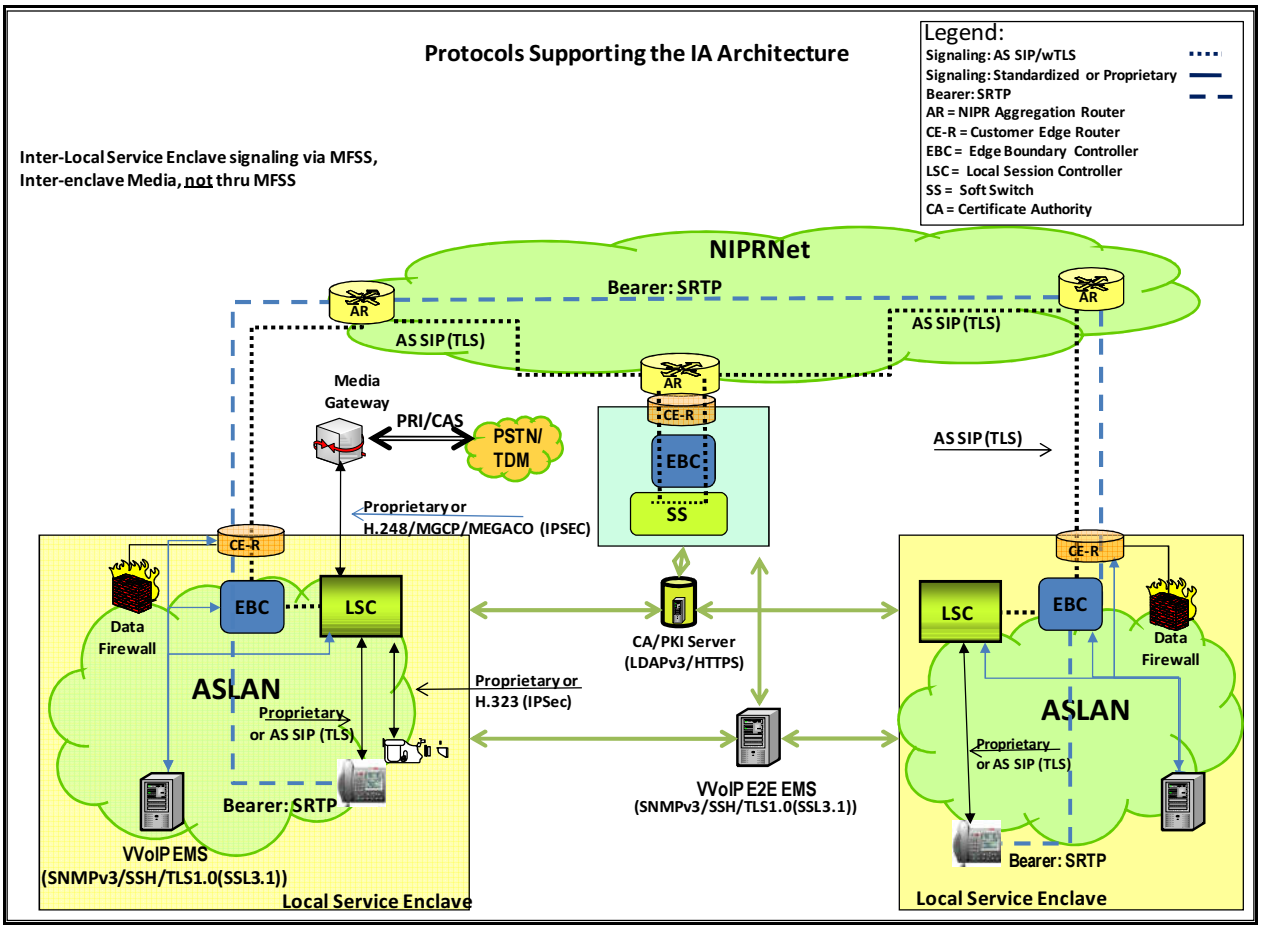

Figure 5.4.5-4. VVoIP Proprietary and Standards Based Protocols

Independent of the protocol or cryptographic algorithm used, many common Information Assurance mechanisms are required of all appliances. For example, every VVoIP signaling appliance that performs a cryptographic function must use a cryptographic module that is FIPS 140-2 level 1 compliant in a FIPS approved configuration (with limited exceptions for certain protocols that are not yet FIPS compliant). In addition, the default encryption algorithm for the VVoIP system is the Advanced Encryption Standard (AES) algorithm with 128-bit encryption unless the protocol does not support AES, in which case the encryption algorithm selected must use 128-bit encryption as a minimum. The default hash is the Secure Hash Algorithm (SHA) – 1, which is supported on every protocol used in this system. However, given the NIST directives to migrate to SHA-256 for digital signatures by 2013 and the direction DoD approved Public Key Infrastructures are heading with respect to SHA-256, as of UCR 2010, all UC devices will need to minimally support SHA-256 when validating signatures on objects generated by ~~the~~ DoD approved ~~Public Key Infrastructures (~~PKI~~).~~ In compliance with DoD requirements and policies, ~~most~~ all VVoIP appliances ~~will~~ are also required to be Public Key Enabled (PKE) so that they may interoperate with the DoD approved PKIs. This~~,~~ directive now includ~~inges with~~ the ~~exception of the~~ EI~~,~~ ~~for~~ which ~~the~~ is required to be DoD ~~PKI~~PKE enabled as of UCR 2010~~PKE requirement is an objective requirement for this iteration of the UCR and will become required in~~

~~UCR 2010~~. ~~Note that the DoD PKI is quickly moving towards issuing DoD PKI certificates that utilize the SHA-256 algorithm (even though as an interim step, some DoD PKI CAs may continue to use SHA-1 until new SHA-256 CAs are established). This exception does not apply to the AEI, which shall be PKE and shall interoperate with the DoD PKI.~~

5.4.5.4.2 ~~End Instrument~~EI Authentication and Registration

The first step in the VVoIP protocol design is the registration of the appliance to the network and its receipt of an E.164 telephone number if it is an EI or a AEI. During the initial installation of an appliance either it will be configured with a static IP address (i.e., LSC, SS, MG, MFSS, AEI, and EI) or will receive its (EI or AEI) IP address from a DHCP server. The first step is for the EI or AEI to authenticate itself to the LAN switch to which it is physically connected using the 802.1X protocol. If DHCP is used, when the EI or AEI authenticates itself to the DHCP server to get its IP address it will also obtain the registration information necessary to locate the LSC. If an EI uses static IP addresses, it will be preconfigured by the system administrator with the location information of the LSC. It is important to note that the DHCP server must be physically separate from the routers and LAN switches. The EI or AEI will then authenticate itself to the LSC so that it may obtain its E.164 number and the LSC shall update its user database and local directory to reflect the active status of the EI or AEI with its associated profile. In addition, the LSC shall authenticate itself to the EI or AEI. The mutual authentication between the EI and the LSC shall be provided through the use of a ~~DoD PKI~~ certificate issued from a DoD approved PKI ~~use~~ in conjunction with a protocol such as TLS or its equivalent ~~for authentication as a minimum and more sophisticated authentication mechanisms, such as a PKI certificate, are encouraged~~. The mutual authentication between the AEI and the LSC shall also use device ~~DoD PKI~~ certificates issued from a DoD approved PKI, but only in conjunction with TLS. Each EI and AEI shall be issued a device DoD PKI certificate ~~and will have~~which will contain a unique Common Name in the X.509v3 Subject field. At this point, the EI or AEI is able to support VVoIP sessions at the ROUTINE precedence level. It is important to note that the exact approach used for proprietary EIs to mutually authenticate with their LSC using PKI certificates is beyond the scope of this document. Figure 5.4.5-5, AEI Registration Process (DHCP), shows the AEI registration process if DHCP is used for obtaining its IP address. The figure simplifies the TLS authentication process for ease of understanding the sequence, but Figure 5.4.5-7, AS-SIP TLS Authentication Process, provides a detailed description of the process.

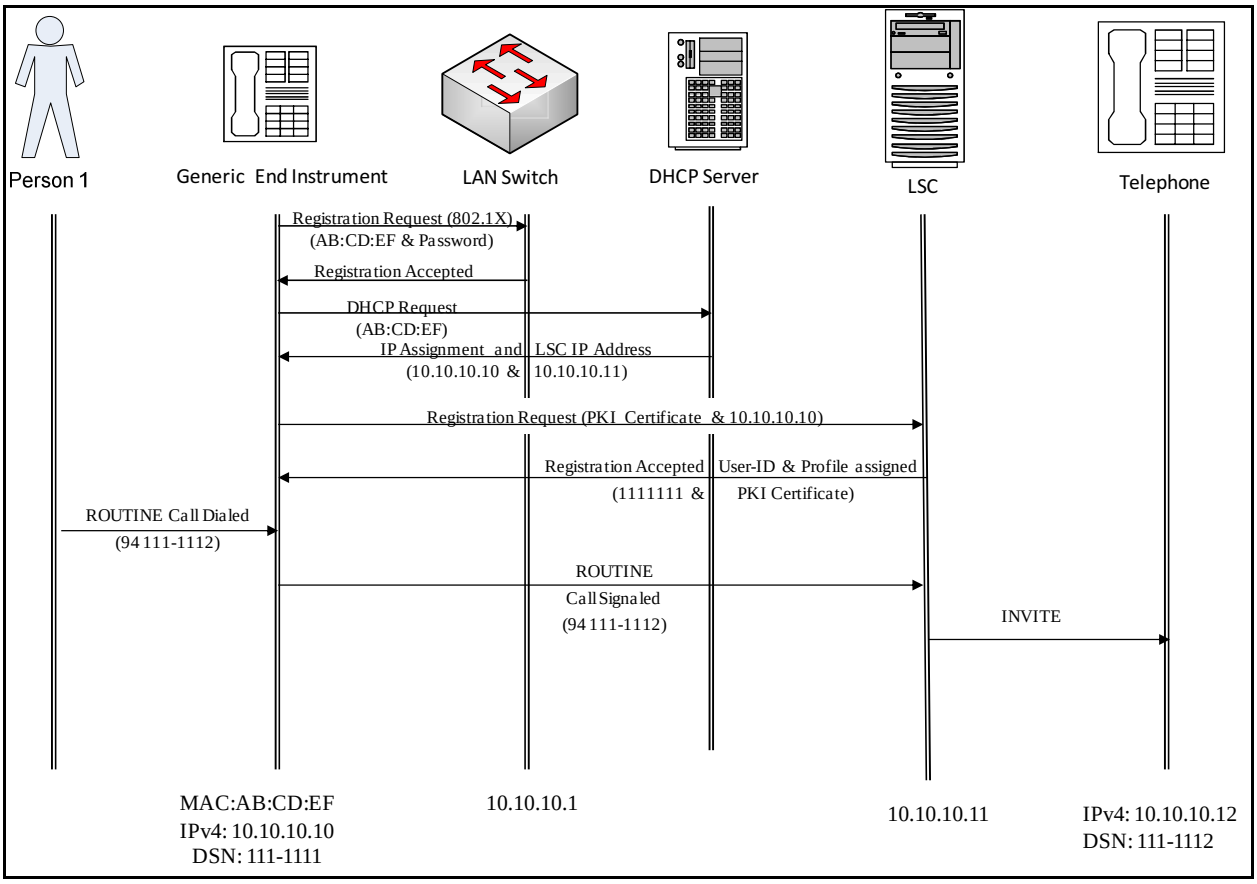

Figure 5.4.5-5. AEI Registration Process (DHCP)

5.4.5.4.3 User Authentication and Authorization

For a ROUTINE precedence VVoIP session, the system does not require user authentication. However, VVoIP sessions above ROUTINE precedence may require user authentication and that authentication may be provided using a User ID (PIN) with an associated numeric password (PIN) or using ~~DoD PKI~~ user certificates issued from a DoD approved PKI. If the end instrument is a softphone, the end instrument should be able to pass the user credential provided by the CAC or other DoD approved token to the LSC for user authentication. If a DoD approved X.509v3 ~~PKI~~ certificate is used, then the certificate path should be authenticated up to the trust point (or anchor point). Alternatively, i~~I~~f no other intermediate trust point is established, the certificate path shall be authenticated to the root certificate or CA. Limiting the authentication of a user to sessions with precedence above ROUTINE also limits the impact that authentication has on the post-dial delay, since the validation of a DoD PKI certificate can take up to 4 seconds to complete. If the user certificate cannot be validated due to an inaccessibility ~~of the On-Line Status Check (OSC)~~to access an online revocation status checking system such an Online Certificate Status Protocol responder, the session setup shall continue, but the event shall be logged and an alarm shall be sent to the NMS.

Based upon the user authentication and the profile associated with that user, the LSC will make a decision on whether to allow the session setup to continue.

Figure 5.4.5-6, Precedence Session User Authentication and Authorization, shows the PKI user authentication and authorization process for session requests above the ROUTINE precedence level.

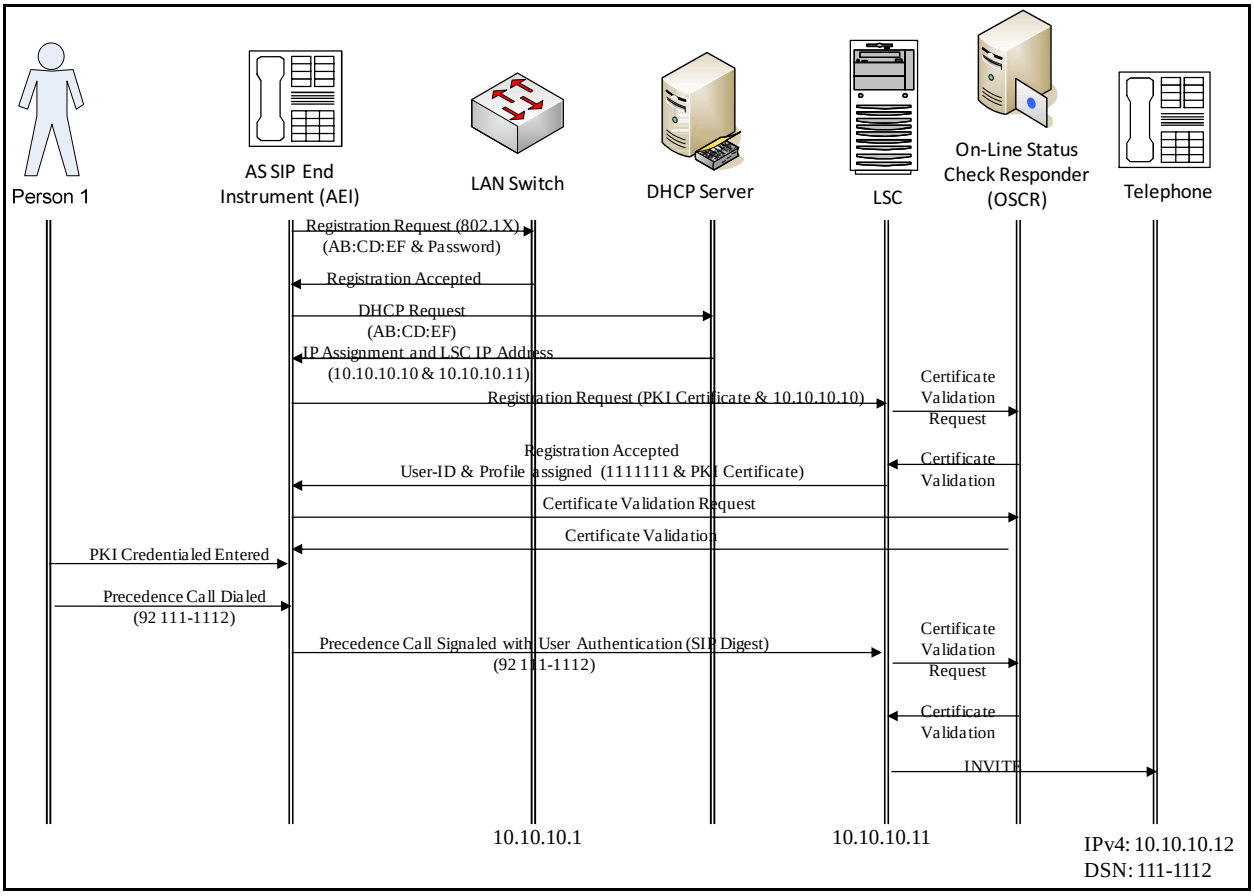

Figure 5.4.5-6. Precedence Session User Authentication and Authorization

5.4.5.4.4 Signaling Appliance Authentication and Authorization

5.4.5.4.4.1 AS-SIP

In addition to user authentication and- appliance authentication, the signaling appliances must also mutually authenticate to each other using a DoD approved PKI~~the DoD PKI~~. Since all signaling appliances support AS-SIP, the authentication mechanisms must be integrated with

AS-SIP in order to provide interoperability. Unfortunately, the SIP protocol is not intended to be a secure protocol and must rely on other security protocols for its security. Since the AS-SIP model chosen is a hierarchical signaling model, TLS was chosen as the Information Assurance protocol to secure AS-SIP since its hop-by-hop security model integrated nicely with the hierarchical signaling model. Fortunately, all AS-SIP signaling appliances ~~(Required in UCR 2010 for an EI, Required for AEI)~~ are required to be DoD PKE and support the ~~DoD PKI~~interoperability with a DoD approved PKI. Currently, t~~T~~he process for obtaining a DoD ~~PKI~~ approved X.509v3 certificate is a manual process and has to be completed before or during the initial installation. ~~The~~ Use of a certificate from a DoD approved PKI, in combination with TLS, provides a secure process for signaling appliances to authenticate to each other and the process must be completed before transmitting an AS-SIP signaling session to the remote AS-SIP signaling appliance. UCR 2010 incorporates new requirements that detail specifically how this validation process, using certificates and AS-SIP signaling messages, must occur.

Figure 5.4.5-7 shows the process that must be completed before AS-SIP signaling is transmitted between AS-SIP signaling appliances.

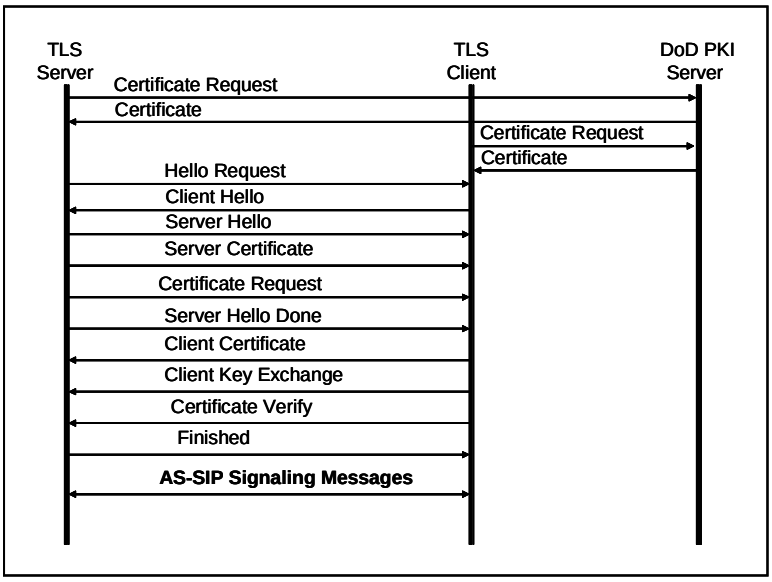

Figure 5.4.5-7. AS-SIP TLS Authentication Process

Once a TLS session is established between the AS-SIP signaling appliances, the AS-SIP signaling messages are allowed to transit between the appliances if the appliance profile permits. Every signaling appliance in the path of a AS-SIP signaling session (with the exception of the EI, where it is Conditional) is responsible for receiving the AS-SIP packet, decrypting the packet, verifying the integrity of the packet, processing the packet in accordance with the AS-SIP specification, and then encrypting the packet before transmitting it to the next hop. Figure 5.4.5-8, AS-SIP Signaling Appliance Packet Processing, shows this process.

5.4.5.4.4.2 H.323 and H.248

Several legacy protocols must be supported until the UCR ~~2010~~ 2012 timeframe. They include H.323, which is primarily used to support video sessions, and H.248, which is primarily used to communicate between a media gateway controller and a media gateway. ~~UCR 2010 also introduces the concept of a remote MG controlled, also using H.248, but tunneled securely across the WAN.~~ The LSC may interpret H.323 and H.248 for line side connections (within a local domain or to the PSTN), but will translate the signaling to AS-SIP for trunk side (WAN) signaling. If H.323 is used for trunk (WAN) side signaling it will involve a point-to-point signaling session that will bypass the LSC and extend directly to the remote EI or Multipoint Control Unit (MCU). TLS can be used to secure H.245 channels within the H.323 protocols because it uses TCP. However, H.323 is also composed of H.225.0 and RAS protocols and these protocols are not compatible with TLS if they are implemented with UDP since TLS requires a reliable protocol (TCP or SCTP). As a result, IPSec was chosen as the protocol to secure H.323 and H.248 and this is in accordance with the DISA FSO VVoIP STIG Checklist.

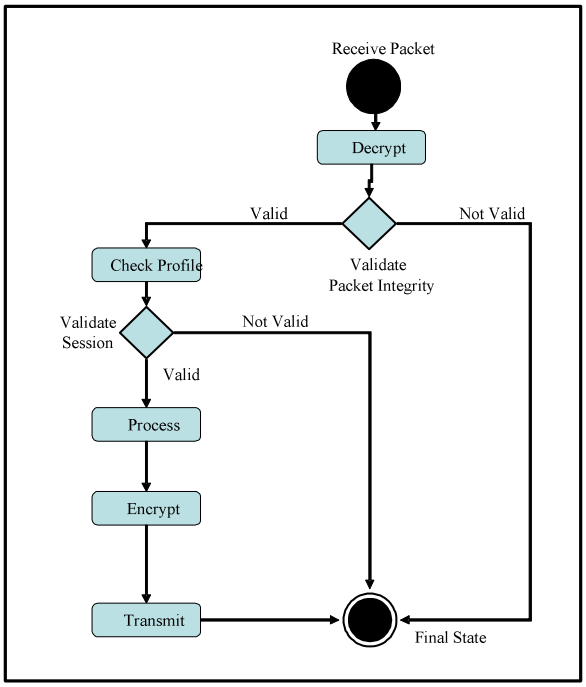

Figure 5.4.5-8. AS-SIP Signaling Appliance Packet Processing

The mechanism used for H.323 authentication and key exchange is the Internet Key Exchange (IKE) protocol. The IKE is a standards-based approach developed by the IETF to support IPSec. The IKE is a method for establishing a security association (SA) that authenticates users, negotiates the encryption method, and exchanges the secret key. The IKE is derived from the ISAKMP framework for key exchange and the Oakley key exchange technique, IKE is designed to support a PKI like infrastructure, such as the DoD PKI.~~,~~ ~~and~~ IKE also has mechanisms to

provide the secure transmission of the secret key to the recipient so that the encrypted data may be decrypted at the other end.

5.4.5.4.4.3 Secure Bearer Path

In addition to securing the VVoIP signaling path, the VVoIP bearer path for EIs is also secured using the SRTP to provide confidentiality and integrity. Since the end-to-end signaling path was authenticated using TLS and the EIs are the origination and termination points for that path, the EIs authentication will be achieved via that hop-by-hop authentication. It is understood that a limitation of hop-by-hop authentication model is that it is only as strong as the weakest link. To understand the effect of this approach, an analysis was conducted that weighed the risk of a hop-by-hop security model with the benefit of reducing post dial delay by eliminating the point-to-point authentication process between the EIs using the authentication provided by the TLS process. The result of the analysis was that the benefits outweighed the risks. Given that additional authentication is not required, the next concern is to reduce the delay associated with exchanging encryption keys.

This was accomplished by embedding the SRTP encryption key for the session in the AS-SIP INVITE message as part the SDP within the AS-SIP packet in accordance with RFC 4568, "Session Description Protocol (SDP) Security Descriptions for Media Streams". H.248 is also capable of distributing the SRTP encryption key in the SDP portion of the H.248 using the same parameter. H.323 distributes the session key in the same manner using the H.235 key distribution mechanisms instead of using SDP. Since the AS-SIP messages are encrypted and checked for integrity, the inclusion of the SRTP encryption key in the AS-SIP message provides a secure method for key exchange. In addition to providing a secure method for transport of the session key, it also allows the encrypted bearer stream to be transmitted as soon as the session setup is complete. The SRTP is used for both confidentiality and integrity of the bearer path. In determining the size of the hash needed to provide SRTP integrity, a cost benefit analysis was conducted that weighed the cost for each SRTP packet to process the hash and the IP overhead associated with the hash with the risk mitigated by a applying a larger secure hash. The analysis showed that a small hash (32-bit) was adequate to mitigate the risk given the large number of packets and the documented threats.

5.4.5.4.5 Network Management

Network management protocols are the final category of protocols that must be secured within the VVoIP environment. Since the Information Assurance architecture leverages the DoD PKI for authentication, it is expected that all EMS personnel will be assigned a CAC or other DoD approved token and will use ~~a CAC~~this credential for authenticating to the system. Once authenticated to the system using PKI, it is expected that the ~~CAC~~ credentials from the token will be passed to the system to provide role-based access to the EMS based on the privileges assigned to the EMS personnel (in other words, no secondary username or password should be required

for authorization purposes). Network management protocols for the purposes of this discussion are separated into two categories dependent on whether they support traditional FCAPS (Fault, Configuration, Accounting, Performance, Security) related functions or directory services type functions. At this time, the VVoIP Information Assurance Design has not identified a requirement for the VVoIP systems (i.e., LSC, SS, MFSS, EBC, CE Router) to interface the EMS using XML-based Web services and this UCR does not address the mechanisms that would be used to secure those services. Although the VVoIP systems do not use XMP-based web services, the EMSs managing the VVoIP systems do utilize XML-based services for Information Sharing and have secure ways of providing the service. The Information Assurance approach used for the Information Sharing is not within the scope of this UCR. Appliances performing network management functions (i.e., LSC, SS, MFSS, MG, ADIMSS, ARDIMSS, etc.) will use static IP addresses and they will not be assigned IP addresses by a DHCP server. Since the IP address can be published to the FCAPS personnel in advance, the session initiator will use the appropriate IP address (either IPv6 or IPv4) in their request and IPv4/IPv6 translation is not required between the terminal and the appliance.

The VVoIP Information Assurance Design requires that every LSC and MFSS support a minimum of two Ethernet interfaces (to include redundancy on each interface). The two Ethernet interfaces are used to support 1) Signaling and Bearer Traffic and 2) the EMS. Using Information Sharing, the EMS (Local or RTS EMS) will share FCAPS information with other EMSs to provide end-to-end management.. Since there are multiple interfaces, the appliance must ensure that traffic transiting from one Ethernet interface to a different Ethernet interface is limited to authenticated and authorized traffic. For example, the LSC appliance must ensure that a user who has access to the signaling and bearer interface to establish a session is not allowed access to the Local EMS network. An instance of transiting between interfaces occurs when a authenticated and authorized systems administrator logs into a LSC in order to perform call tracing functions as part of a trouble shooting sequence. In this case, the system administrator entered the system through the EMS interface, but transmitted the traffic through the- signaling and bearer interface. The external Ethernet interfaces are assigned to distinct VLANs in accordance with the types of traffic they support. Figure 5.4.5-9, VVoIP Product External Ethernet Interfaces, shows an example of the Ethernet interfaces found on an LSC and the access controls that may be configured to control traffic between the interfaces.

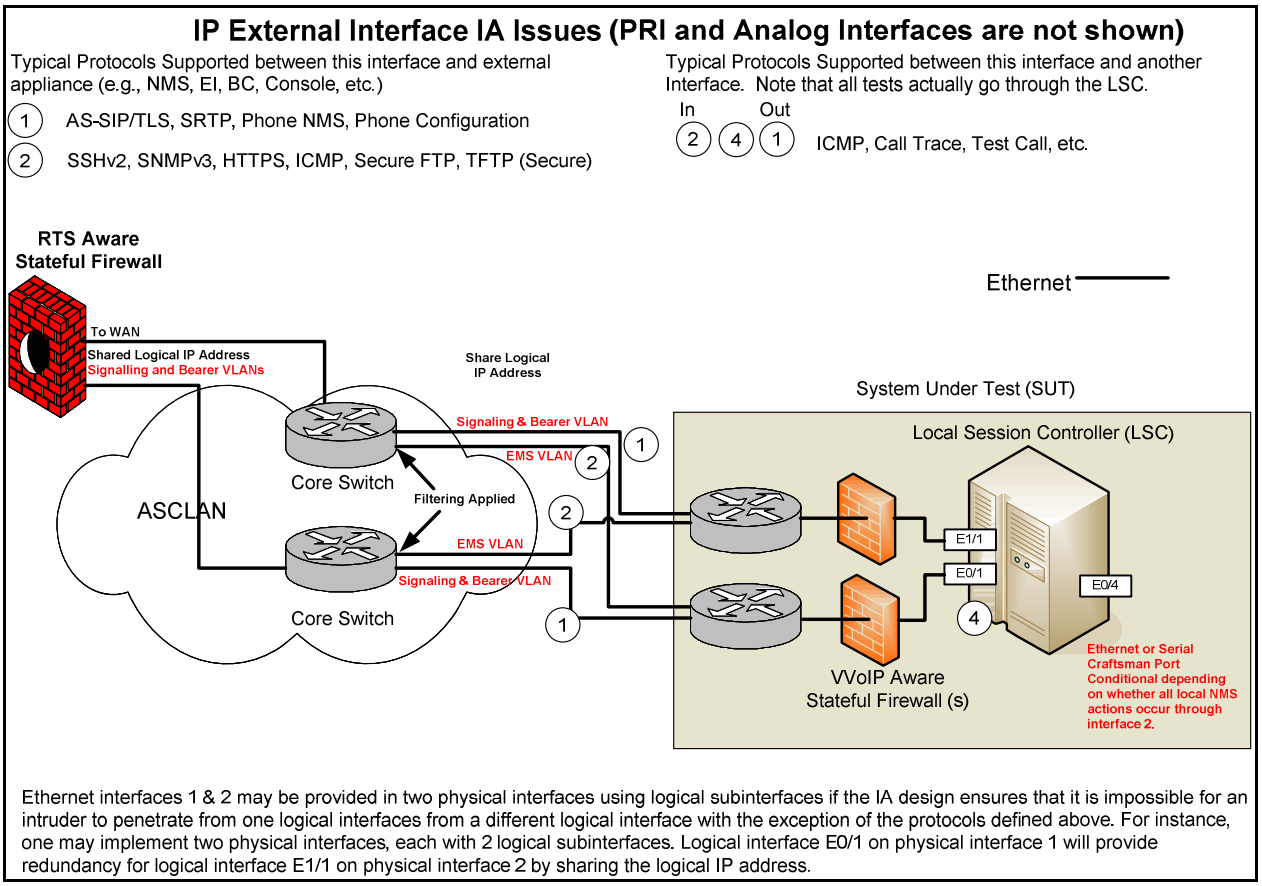

Figure 5.4.5-9. VVoIP Product External Ethernet Interfaces

The first category of protocols is the protocols that support FCAPS. These have been defined as the SNMPv3, the SSHv2, and Secure Sockets Layer (SSL) Protocol version 3.1. SNMPv3 builds upon earlier versions of SNMP, but adds additional security mechanisms that are integrated into the protocol. SNMP is primarily used for minor configuration changes and for providing real time status on the VVoIP appliances. The VVoIP Information Assurance Design requires the use of SNMPv3 as a threshold requirement due to its significant improvement in the Information Assurance area over previous versions. However, it is understood that due to its newness, some solutions may have to use earlier versions of SNMP with the mitigations of the appropriate patches, IPSec, and an upgrade plan for migrating to SNMPv3 due to their development cycles. The VVoIP Information Assurance design will use the SNMPv3 User Based Security Model.

SSHv2 is defined in RFC 4251 as a protocol for secure remote login and other secure network services over an insecure network. Primarily, SSHv2 is in the DoD VVoIP environment as a secure configuration and control protocol used by network engineers to access network elements in order to configure the appliances. It should be noted that EIs and AEIs will disable remote manual configuration after the initial installation is completed and should not allow remote manual configuration after the initial installation. In addition, all EI and AEI non-automatic processes shall be performed locally. The SSH protocol consists of the following three major

components: the Transport Layer Protocol, User Authentication Protocol, and Connection Protocol. The Transport Layer Protocol provides server authentication, confidentiality, and integrity. The User Authentication Protocol authenticates the client to the server, and the Connection Protocol multiplexes the encrypted tunnel into several logical channels. UCR 2010 now requires all SSHv2 implementations to support the transmission of full X.509v3 certificates during session establishment.

The final protocol is the TLS, version 1.0 or higher, which for the purposes of this design is considered interchangeable with SSL, version 3.1. The SSL is used within the network management system as an alternative to SSHv2 and is primarily associated with web-based network management GUIs. It provides a secure manner for authorized and authenticated network engineers to access VVoIP appliances to perform network management functions.

The second category of network management protocols is associated with location services. Lightweight Directory Access Protocol, version 3 is the protocol that will be used to interface between the RTS Routing Database and the LSC and SS. In addition to directory services, LDAPv3- mayis also be used to support interface with portion of the DoD PKI and is designed to provide access to directories supporting the X.500 models, while limiting the resource requirements associated with other protocols. The LDAPv3 is specifically targeted at management applications, such as the DoD PKI and directory services that provide read/write interactive access to directories, including accessing stored PKI certificates and E.164 addresses. When used with a directory supporting the X.500 protocols, it is intended to be a complement to the X.500 Directory Access Protocol (DAP). The LDAP is nothing more than an access protocol and does not require the underlying directory database to be based on any particular technology. The LDAPv3 is designed to integrate with TLS in a similar manner to AS-SIP. The TLS is used with LDAP to provide confidentiality, integrity, and authentication in combination with the use of the DoD PKI certificates. The use of TLS does not provide or ensure confidentiality and/or non-repudiation of the data housed by an LDAP-based directory server, nor does it secure the data from inspection by the server administrators. Once established, TLS only provides for, and ensures confidentiality and integrity of the operations and data in transit over the LDAP association and only if the implementations on the client and server support and negotiate it.

5.4.5.4.6 AS-SIP End Instruments

End instruments can be placed into two broad categories on the basis of the signaling protocols that are used to communicate with the LSC to set up the call. These categories are “vendor proprietary” and “AS-SIP”.

EIs are end instruments that use vendor-proprietary signaling interfaces between the LSCs and itself. Both ITU H.323 and IETF SIP (commercial SIP, not DISA-specified AS-SIP) are also considered vendor-proprietary EI to LSC protocols in this UCR 2008. They are treated as

vendor-proprietary protocols because one EI vendor's implementation of H.323 or SIP is not guaranteed to interoperate with another LSC vendor's implementation of H.323 or SIP.

AEIs~~AEIs~~ are end instruments that use AS-SIP between the LSCs and AEI itself. AEIs from any AEI vendor operate on any LSC vendor's product, using the AS-SIP-based LSC-to-AEI interface.

5.4.5.4.6.1 Secure VVoIP End Instruments

Secure EIs are NSA Type-1 certified VVoIP terminals that support the end-to-end transmission of classified VVoIP media traffic. Secure EIs can also be placed into "vendor proprietary" and "AS-SIP" categories on the basis of the signaling protocols that are used to communicate with the LSC to set up the call.

The IP secure EI is currently designed to rely on the SCIP standard~~, that was adopted as the replacement for the (T~~the FNBDT standard was renamed SCIP in 2004). The IP secure DSCD ~~will rely~~relies on SCIP transported over either V.150.1 or SRTP on the IP network to ~~provide~~ transmit classified voice and data across the DoD IP networks. NSA has directed that IP DSCDs adopt the AS-SIP protocol as the default VVoIP signaling protocol.

5.4.5.4.7 Edge Boundary Control Appliances

The VVoIP Information Assurance design uses two appliances to defend the boundary between the Customer Edge Segment and the Network Edge Segment. The first appliance is called the EBC and its function is to act as a VVoIP aware firewall. The second appliance is called the CE Router, and its primary functions are associated with QoS and perimeter defense. Figure 5.4.5-4, VVoIP Proprietary and Standards Based Protocols, shows the location of the EBC and the CE Router. Both appliances must be highly reliable (i.e., 99.999 percent available) and IPv6 capable using a dual stack.

The CE Router is responsible for providing traffic conditioning (policing and shaping) on inbound and outbound traffic to ensure that the performance requirements are met for both the Network Edge Segment and the Customer Edge Segment. This is one of the defense-in-depth mechanisms used to prevent a Denial-of-Service (DoS) attack by ensuring that only a predetermined number of signaling or VVoIP sessions may transit the CE Router at a particular instance of time. It is understood that this only prevents the Customer Edge Network from being impacted by a DoS attack and that the external connectivity may be affected. The granularity of the traffic conditioning is to the level of the granular service class, such as voice or video. Currently, the configuration changes associated with traffic conditioning will be a manual process. However, it is hoped that the Fiscal Year (FY) 2012 Design will incorporate dynamic traffic conditioning based on policy. To achieve this vision, an interface must be defined for communication between the AS-SIP signaling appliance (i.e., LSC or SS) and the CE Router in

order to ensure that the AS-SIP signaling appliance budgets are consistent with the CE Router traffic conditioning parameters. In addition, the CE Router must also have the capability to provide QoS for VVoIP by supporting the Per-Hop Behaviors (PHBs) based on the DSCP markings that will be defined by the QoS Working Group.

Primarily, the EBC is focused on perimeter defense. Real time services suffer from certain difficulties with traditional perimeter defense mechanisms, such as NAT and data firewall behavior. Many protocols designed by the IETF used within the VVoIP environment, such as SIP, are designed as end-to-end protocols. The end-to-end model is broken by the presence of firewalls and NAT appliances. In large deployments of VVoIP, such as the DISN, a specialized appliance is needed to facilitate the coexistence of VVoIP and perimeter defense mechanisms. The DoD VVoIP Information Assurance design has labeled this specialized appliance as an EBC to distinguish it from similar commercial appliances that do not have unique DoD requirements. Before describing the requirements and functions associated with the EBC, it is important to explain the difficulties that VVoIP protocols experience crossing network boundary devices and to explain the common types of solutions available in the commercial market that leverage commercial standards. Following this discussion, a general discussion of the requirements associated with an EBC will be provided.

As mentioned previously, the use of NAT introduces several problems to an end-to-end protocol security model. The use of NAT is required at the WAN boundary by the VVoIP and Network Infrastructure STIGs. In a traditional NAT employment, the NAT is conducted at the Network Layer (Layer 3) of the OSI model (Network Address Port Translation is conducted at Layer 4). However, the DoD VVoIP environment requires that the EBC perform NAT at a higher layer in order to process the AS-SIP messages properly. The common scenario provided for NAT is the use of private addressing in two remote enclaves, with a public address space in the interconnecting WAN.

During the initial AS-SIP offer/answer exchange, both the originating and terminating AS-SIP User Agents (UAs) will specify in the SDP payload the desired IP address and port combination for the caller and called party to receive the associated media stream and to properly direct the signaling stream. AS-SIP UAs within the Customer Edge segment may use private addressing for topology hiding reasons. A problem occurs when private addressing is used within the SDP payload since the private address is not resolvable from the WAN side of the NAT. A traditional NAT device will change the IP source address and/or port combination at packet header level, but not the IP address within the SDP payload. Consequently, the called party, or User Agent in the remote enclave, will not have the correct IP address to respond to from a signaling perspective and the call setup will fail. Even if the call is established from a signaling perspective, the bearer stream would be sent to the wrong address/port and the session would not be established.

An additional problem is that the signaling and bearer paths are different IP sessions and NAT bindings in a traditional NAT appliance are finite in nature (not correlated). A scenario may result in that a VVoIP session may continue for many minutes with active RTP streams, but no signaling messages. Since there is no signaling, the signaling NAT binding could time out, and the session would not be able to end properly.

Difficulties experienced by AS-SIP signaling and Real Time Protocol/Real Time Control Protocol (RTP/RTCP) media protocols passing through firewalls stem mainly from the fact that bearer stream port numbers are selected dynamically for each call from a large pool of potential port numbers. Allowing this large range (typically around 20,000 UDP ports for a large MILDEP) of potential port numbers to be open at the enclave boundary is unacceptable. The EBC needs to know which ports to open temporarily, when to open them, and when to close them. Placing this functionality (essentially an Application Level Gateway) into data firewalls is slow to occur in the commercial market and carries with it some disadvantages, for example, having the firewall perform actions it is not supposed to handle.

Solutions for these issues have evolved slowly within the standards bodies and major equipment vendors. A myriad of suggestions have been offered from both communities, yet none has attained widespread acceptance. Efforts have included work from the IETF's Middlebox Communication (MIDCOM) Working Group, which closed in March 2008. The envisioned MIDCOM Design provided for a protocol link between the LSC and the boundary device, a firewall or NAT device, called a middlebox, for the purposes of opening and closing pinholes in the middlebox. The MIDCOM Working Group never completely achieved its goal, but certain pre-MIDCOM solutions, such as Simple Tunneling of UDP through NAT (STUN) and Interactive Connectivity Establishment (ICE), have been implemented in freeware projects and in some products. Widespread deployment of technologies such as STUN, Traversal Using Relay NAT (TURN), and ICE has not happened as of this writing. In the interim, some vendors have developed limited solutions for their products to allow functionality, and several have acquired EBC functionality to enhance their product lines, however, no clear solution to achieve multivendor interoperability has come out of the major vendor arena. As a result, interoperability problems often occur between different vendor solutions due to the proprietary nature of the vendor unique solutions.

Some of the difficulty with solutions coming from the standards arena is an aversion to dealing with middleboxes at all. NAT was originally meant to be a short-term solution to the IP address depletion problem. Many Application protocols are designed to be end-to-end in nature, and firewalls and NAT devices break this end-to-end nature of many protocols. There are also arguments that middleboxes prevent application layer protocols from protecting themselves by breaking the end-to-end security model. Standardization of NAT behavior has not occurred and has resulted in NAT implementations that behave differently from vendor to vendor. Another IETF working group, the Behavior Engineering for Hindrance Avoidance (BEHAVE) working

group, was formed to identify, classify, and understand these behaviors in order to bring some standardization to them but the end state of a standardized behavior has not been achieved.

In response to a need for a solution to various problems with VVoIP in the areas of firewall/NAT traversal, topology hiding, and lawful intercept, a large number of startup companies have produced a solution that has come to be known as Session Border Controller (SBC). These products may provide functionality in one or more areas, however there is no standardization among the producers of these products and they currently do not meet the DoD unique requirements associated with the processing of AS-SIP, so it is necessary for the DoD to specify precisely the functionality required in these solutions.

The result of this situation is that the DoD has defined an EBC system that is placed at the boundary between the Edge segment and the Access segment to provide ~~three~~ four critical functions; topology hiding, "pinholing," ~~and~~ filtering, and as of UCR 2010 VVoIP traffic monitoring.

Topology hiding is accomplished by processing the AS-SIP messages and performing the appropriate IP address and port translations within the IP header and the SDP payload. Figure 5.4.5-10, Typical End-to-End AS-SIP Call Flow, shows the typical call flow associated establishing an AS-SIP session. The diagram shows how the media is bi-directionally anchored by the EBC to ensure that topology hiding is provided in accordance with the DoD requirements.

Several issues are encountered by EBCs in attempting to meet the topology hiding requirements due to the VVoIP signaling hierarchy and by the requirement to allow call forwarding and call transfer. The first issue is found in EBCs that front a Softswitch component of an MFSS. Upon receipt of an AS-SIP INVITE, the EBC does not know whether that session terminates within the enclave, or will be forwarded to another enclave (after processing by the Softswitch). Due to the uncertainty, the EBC must anchor the media stream bi-directionally. If the Softswitch returns the INVITE to the EBC for forwarding to the next hop, the EBC must restore the original IP address and port number so that it is no longer involved in the media stream associated with that session.

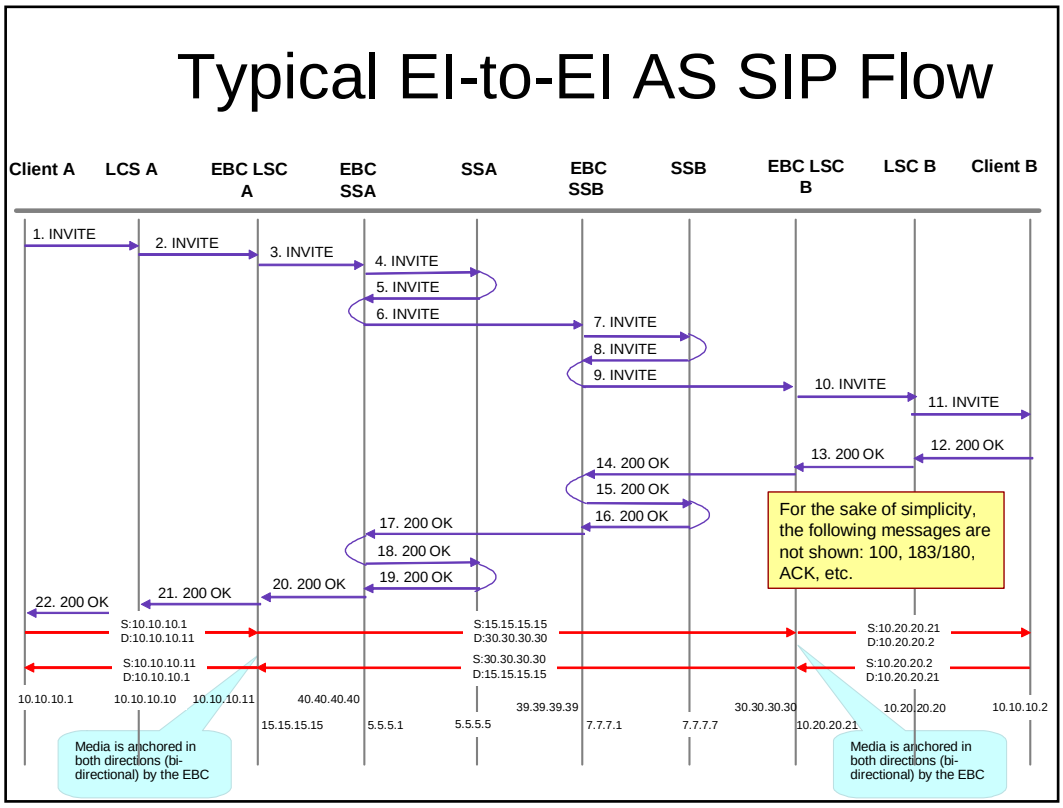

Figure 5.4.5-10. Typical End-to-End AS-SIP Call Flow

Figure 5.4.5-11, Media Anchoring for Transitive SIP Signaling, shows the process associated with transitive SIP signaling for an EBC that fronts the Softswitch component of the MFSS.

The second issue associated with topology hiding is related to call forwarding and call transfer scenarios where the session no longer terminates within the enclave. Upon notification that a session is being forwarded or transferred, the EBC associated with the forwarding or transferring party must restore the original IP address and port number associated with that session to ensure that the media is not improperly anchored at the enclave since the session is no longer associated with the enclave. The process used is similar to the process described in Figure 5.4.5-11~~Figure 5.4.5-10~~, Media Anchoring for Transitive SIP Signaling.

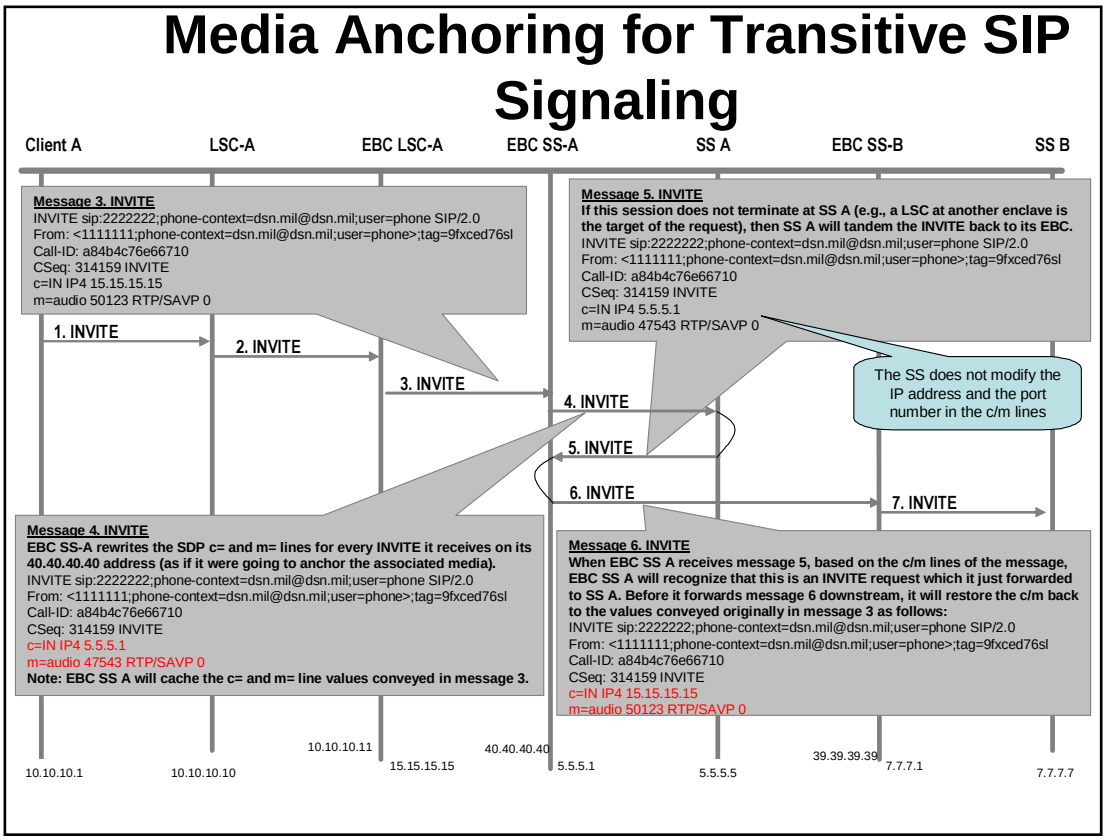

Figure 5.4.5-11. Media Anchoring for Transitive SIP Signaling

The next issue concerns the ability of the EBC to determine the appropriate next hop for signaling. For an EBC fronting an LSC, the EBC has only a primary and secondary TLS path in which to forward the AS-SIP messages. The primary TLS path is to the EBC fronting the primary MFSS for the LSC and the secondary path is to the EBC fronting the secondary MFSS for the LSC. However, for an EBC fronting the Softswitch component of the MFSS, it has numerous TLS sessions associated with the subtended LSCs of the MFSS and with the other Primary and Secondary MFSSs for all the remote LSCs. Since the EBC does not have its own location service, it must rely on the Softswitch component of the MFSS to inform it of the appropriate next hop. The Softswitch informs the EBC of the next hop using the Route Header construct defined in the RFC 3261. It is important to note that this issue is not relevant to INVITEs arriving from the WAN, since the EBC is associated with one and only one AS-SIP signaling system on the line side and always forwards INVITEs arriving from the WAN to its associated AS-SIP signaling system (i.e., LSC or MFSS). In addition to performing topology hiding, the EBC provides several other functions to include "pinholing."

"Pinholing" is accomplished by opening and closing "pinholes" that only allow approved sessions to transit the EBC based on the AS-SIP messages. The coupling of the signaling and bearer stream requires that both streams must transit the EBC. If H.323 video is also transiting the EBC, the "pinholes" may also be associated with the H.323 messages. In addition, the EBC

must have a timer associated with each "pinhole" to ensure that "pinholes" do not remain open indefinitely if a signaling message is not received to close the "pinhole." If the EBC closes the "pinhole," it must send a BYE message in each direction to notify the next hop signaling appliances that the session has been terminated.

Filtering is accomplished by allowing targeted IP flows to transit the EBC based on their "6 tuple," which in VVoIP consists of the:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- DiffServ Code Point
- Protocol identifier

Compared to "pinholes," filtering is a manual process and is not dynamic in nature. A type of traffic flow associated with filtering is a SNMPv3 session from the EMS to a LSC that is active all the time and is well defined. If the EBC detects an anomalous condition (DoS attack, abnormal number of invalid AS-SIP requests, etc.), it must have the ability to notify the appropriate EMS of the event.

Beginning with UCR 2010, the EBC is also required to provide either an onboard VVoIP specific IDS/IPS capability or an interface to external VVoIP IDS/IPS which can monitor the VVoIP signaling and media traffic for potential threats. The EBC represents the ideal location for such a capability because the EBC is generally the only place in the architecture, other than the endpoints, where signaling and media traffic transit the same component. The VVoIP IDS/IPS does not have to necessarily be a separate, independent, component from the data IDS/IPS already in use at the site provided that the existing IDS/IPS provides the required VVoIP monitoring capabilities. If an external IDS/IPS interface is provided by the EBC, the interface must be secure and must minimally meet the security profiles defined for IPSec and TLS in this UCR.

5.4.5.4.~~7~~8 RTS Stateful Firewall (RSF)

The role of the RTS Stateful Firewall (RSF) is to protect a LSC, SS, or MFSS from attacks that originate from inside of the enclave. The placement of the RFS within the LAN is displayed in Figure 5.4.5-2. In most deployment scenarios the LSC, MFSS, and WAN SS provide a sufficient Information Assurance posture to be deployed without a RSF. Therefore, the use of the RSF is not a mandatory requirement. However, some MILDEPs may determine that additional protection is required because of the risks associated with their unique scenario (i.e., such as a large regional MAN). When this occurs, the RFS may be deployed to provide additional protection. The RSF is similar to a EBC and may be a EBC. However, the RSF is only required

to support a subset of the EBC requirements. For example, the RSF is not required to support NAT and NAPT and is not required to support ROUTE headers to support failover scenarios. The primary requirement that is added to a RSF that is not applicable to a EBC is the support of both TLS dual path and reuse methods. The RSF needs to support both methods since it will be involved in the SIP dialogues between the LSC and the AEIs and the LSC and proprietary SIP EIs. Since proprietary EIs have an option to implement both TLS methods, the RSF needs to support both methods. The EBC is not involved in TLS sessions between the LSC and EIs and only needs to support AS-SIP TLS sessions, which use the dual path method.

5.4.5.4.9 Smartphone End Instruments and Backend Support Systems

In the context of this document, a "Smartphone End Instruement" is defined as an application that provides End Instrument (EI) or AS-SIP End Instrument (AEI) functions. However, unlike a traditional EI, this is an application that operates within the confines of an advanced, mobile computing platform (e.g. a smartphone, PDA, wireless tablet, etc.) which provides functionality beyond just basic telephony services. ~~The following f~~Figure 5.4.5-12 illustrates the relationship between a Smartphone EI and its operating platform.

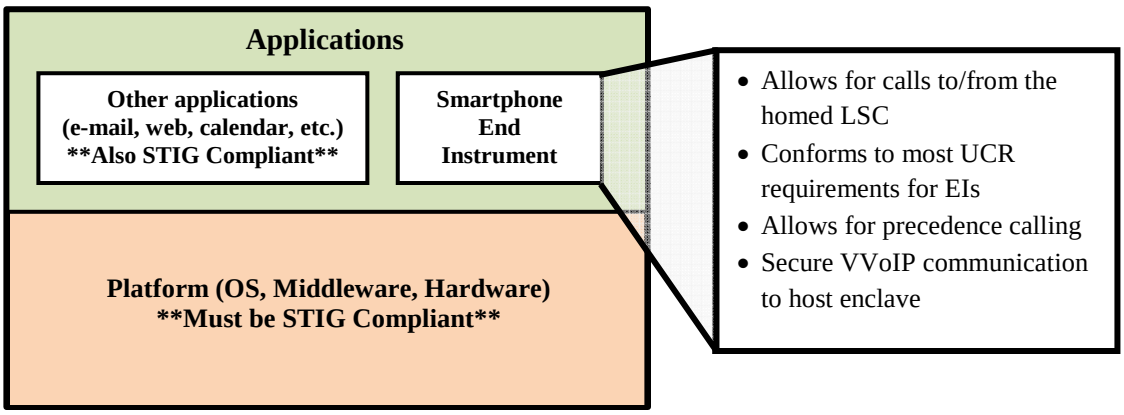

Figure 5.4.5-12: Smartphone End Instrument Relationship to the Host Platform

Even though a Smartphone End Instrument provides functionality similar to a standard End Instrument or AS-SIP end instrument, there are some important differences. First and perhaps most important, a Smartphone EI will typically operate over non-DoD controlled, public access networks to include the public Internet and wireless commercial carrier networks. Also, because public networks in many cases do not provide quality of service and availability guarantees, calls made using a Smartphone EI will not have availability comparable to calls originating from within the VVoIP enclave—in spite of the fact that an assured services VVoIP network is used within the enclave. Lastly, other applications operating on the same platform as the Smartphone

EI could provide any number of e-mail, GPS, Bluetooth, web browsing, instant messaging, or SMS services. These additional services must not weaken the security posture of the device when it connects to the assured services VVoIP network.

The addition of Smartphone EIs to the VVoIP operating environment provides the opportunity for enhanced mobility and connectivty, but also requires the implementation of additional safeguards in order to maintain the security posture of the network. Unlike an EI or AEI, which has nearly direct network layer 3 connectivity to its homed LSC[1], a Smartphone EI is only permited to connect to its homed LSC in one of two ways:

1.) Establish an encrypted VVoIP signaling and media traffic session with a "Back-to-Back User Agent," providing functionality similar to an EBC, at the edge of the homed enclave. This Back-to-Back User Agent communicates on behalf of the Smartphone EI to the homed LSC using the LSC's native, vendor-defined line-side protocol or AS-SIP.

2.) Establish a VPN tunnel to a VPN Server located within the home enclave's DMZ. The VPN server extracts the VVoIP signaling from the VPN tunnel and transmits the information, to the homed LSC. If necessary, a translation step can occur at the VPN server if the information received/transmitted via the VPN tunnel is not already compatible with the LSC's vendor defined line-side protocol or AS-SIP.

~~The following f~~Figures 5.4.5-13 and 5.4.5-14 illustrate these options. For simplicity, required additional security elements such as firewalls and intrusion detection systems, are omitted from these figures.

[1] Though the term LSC is mainly used in this section, an SS or MFSS could also provide the same functionality for a Smartphone EI.

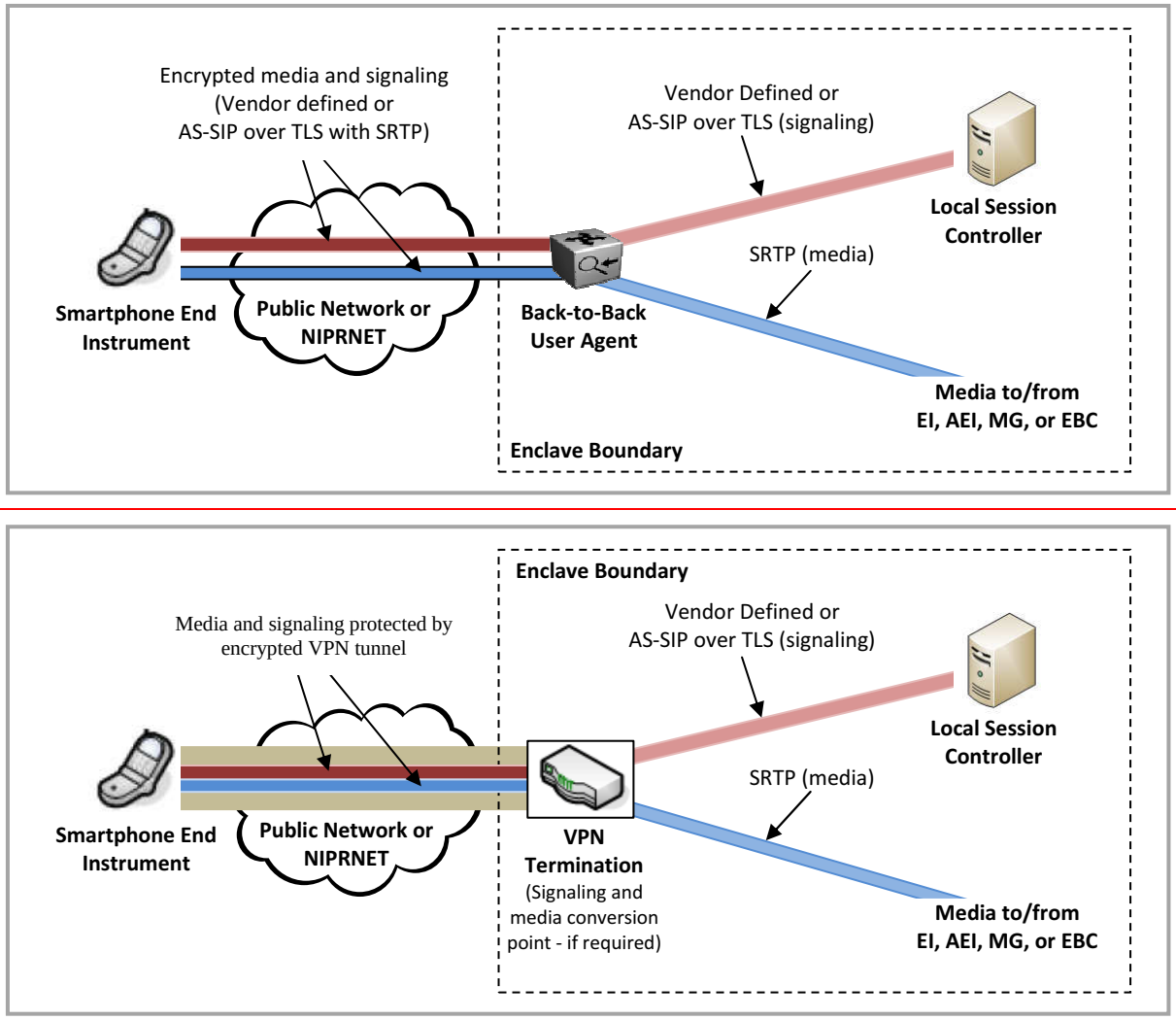

Figure 5.4.5-13: Options for secure LSC connectivity from a Smartphone EI

In general, the specifics of the type of solution and protocols utilized to provide secure LSC connecitivty are left to the discretion of the vendor. However, there are several basic minimum requirements for confidentiality, authentication, integrity, etc. to which the complete system must adhere. The smartphone platform and any supporting servers must meet all applicable requirements contained in any STIG checklists, FSO Security Requirements Matrices and applicable DoD policies. For instance FIPS 140-2, DoD PKI interoperability, mutual authentication, etc. are examples of the required functionality. In addition to these requirements, this UCR defines requirements specific to the Smartphone EI VVoIP application. These requirements range from protecting data at rest to providing providing authenticated remote administration capabilities, in accordance with the STIGs.

Regardless of whether a VPN or Back-to-Back user agent (or both) is used, this document utilizes the term “Smartphone Backend Support System” (SBSS) to represent, in generic terms,

the applications and services used to terminate the secure connection from the Smartphone EI as well as provide management functions.

From an interoperability standpoint, it is anticipated that Smartphone EI vendors will not field directly compatible solutions. However, because the Smartphone EI relies on its homed LSC for session establishment, the LSC will serve as the basis for interoperreability between other AS-SIP devices as well as other devices served by the line-side protocol of the LSC. As a result the Smartphone EI and the Smartphone Backend Support System are considered to be a part of the LSC. This fact impacts how the testing of this system will occur, since the Smartphone EI, the Smartphone Backend Support System, and the LSC will therefore be tested together as a complete system under test (SUT).

~~The following f~~Figure 5.4.5-14 provides a more detailed view of how session establishment would occur between Smartphone EI and a wired End Instrument located within the enclave.

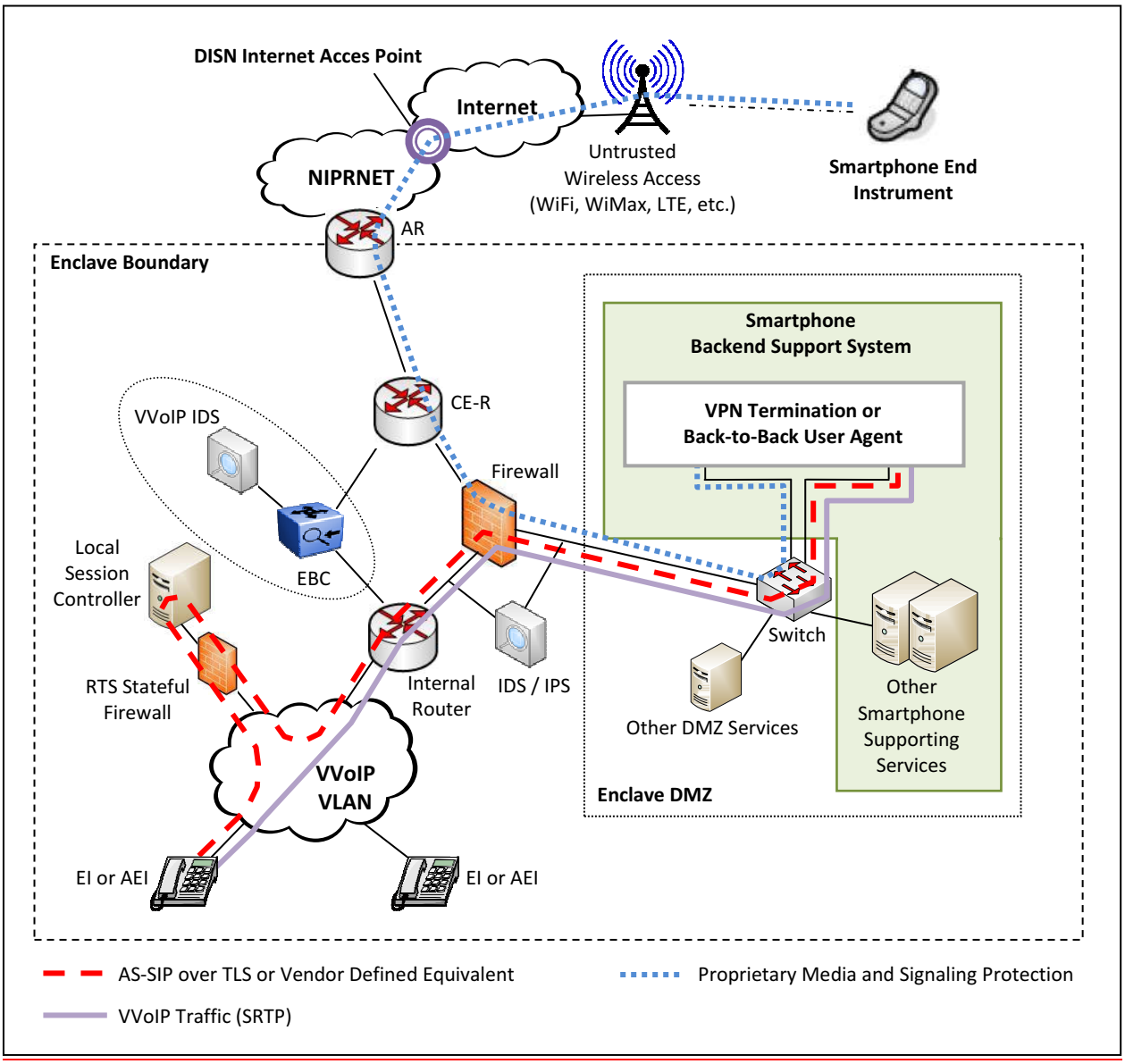

Figure 5.4.5-14: Architecture for Smartphone Access via Untrusted Internet Connection

The figure illustrates placement of the Smartphone Backend Support System within the enclave's DMZ. However, if the system provides back-to-back user agent with dynamic port "pinhole" functionality similar to an EBC, sites may prefer to place the back-to-back user agent in line with the EBC and data firewall rather than behind the data firewall. For simplicity this option was not shown in the figure and could only be implemented if approved and accredited by the site DAA.

The figure also shows a call between a Smartphone EI and an EI or AEI, however the call could just as easily have been routed to the EBC or the MG as appropriate depending on the call source/destination. Regardless, the traffic must be an an "RTS Compliant" format upon entry into the network. In other words, the VVoIP signaling and media must be protected in

accordance with the requirements in Section 5.4 of this UCR and the packets must have appropriate DSCP markings consistent with the requirements in section Section 5.3.3. Since the platform on which the Smartphone EI resides will likely support other applications besides voice, appropriate marking of the Smartphone EI application packets becomes even more important.

The "Other Smartphone Supporting Services" symbol in the figure represents the services that must accompany these solutions, which include authentication of remote devices and checks related to the security posture of the device. These services may also support other non-VVoIP related applications such as e-mail, web browsing, instant messaging, as appropriate. Note that even though the figures show this functionality as being logically separate from the LSC, some vendors may choose to implement certain functions within the LSC rather than as a service provided by an external device.

5.4.5.5 Security Devices

A detailed discussion of UC Security Devices and their functionality occurs in Section 5.8 of this UCR and for brevity will not be repeated here ~~and for brevity will not be repeated here~~. As of UCR 2010, ~~this section~~Section 5.4 now contains information assurance requirements- extracted from Section 5.8 via a phased approach~~that resultinged from the first phase the of extracting IA requirements from Section 5.8 IA requirement extraction~~. A follow-on phase will further harmonize the ~~IA~~information assurance requirements in this section associated with ~~of~~ Security Devices ~~to~~and ~~those of~~ -VVoIP components.

Per a decision from the UC Steering Group, additional Security Devices will be incorporated into later UCR revisions. These new devices include Integrated Security Solutions, IA Tools (Wired and Wireless), and Network Access Control systems. The requirements for these new product types will be incorporated in Section 5.4 and Section 5.8 as appropriate ~~and~~ as requirements for these new product types~~s~~ are developed.

5.4.5.~~5~~6 ~~VVoIP~~ Information Assurance Design Items Outstanding

Several VVoIP Information Assurance design items are outstanding and associated with the uncertainty of the final VVoIP design. Some issues that must be resolved before the completion of the VVoIP Information Assurance design are the finalization of the VVoIP closed loop ASAC solution and the addressing wireless technology Information Assurance issues. In addition, the proper design for securing multicast was deemed too difficult to address in this version of the UCR ~~2008~~ and may be included in future revisions as the DISN multicast design solidifies. Also, full standardization of the exact mechanism by which User credentials from a CAC or other DoD approved token may be standardized in later UCR revisions.

~~The VVoIP Information Assurance Design team has not developed Information Assurance requirements to compliment the softphone requirements of the VVoIP STIG and future revisions of this section will be updated to correct this omission.~~ It is also assumed that the review process of UCR ~~2010~~ 2012 will identify several outstanding Information Assurance items that will need to be addressed in subsequent revisions of this UCR.

5.4.6 Requirements

5.4.6.1 Introduction

To minimize impact to the structure of this section and its associated requirements, the requirements specific to VVoIP components have been kept in their respective sections relative to previous UCR revisions, even though new requirements for Security Devices have been incorporated.

~~Based on~~For the components comprising the ~~VVoIP~~ UC Information Assurance design, a ~~threats and CMs, a~~ set of derived requirements were developed based on the analyzed threats and countermeasures. Different vendors combine different functions into their appliances to meet the requirements of a particular type of product. ~~For the purposes of UCR 2008,~~ T~~t~~he requirements are levied on the individual appliance, as applicable, to secure the entire product. In many cases the system is composed of multiple appliances. For example, an LSC is typically composed of a Call Connection Agent, a media server, a configuration server, a voicemail server, and other servers. Due to the wide variation in vendor products, it is impossible to break out the requirements for each component of a system and the reader should apply the higher level requirements to that component unless specifically stated. An example is that the LSC requirements apply to a media server since it is not specifically called out. However, media gateway and EI requirements are specifically called out and therefore the LSC requirements do not apply to them. The terms user and customer are used in the same context as GR-815-CORE. It is understood that the Information Assurance design provides a high-level description of how the security services are applied to the appliance and how the appliances interact in a secure manner. In addition, the appropriate STIGs will further clarify how the Information Assurance design and requirements are implemented on the appliance. For example, all Security devices would comply with the Application Security and Network Infrastructure STIGs and STIG Checklists.

In general, UCR ~~2008,~~ Section 5.4, Information Assurance Requirements, is intended to provide a level of security requirements consistent with the level of security requirements specified in the GR-815-CORE, but adapted for the unique DoD ~~VVoIP~~ UC environment and consistent with the requirements in the UCR.

~~To assist the reader in the origin of the requirements, Information Assurance requirements are broken down according to the reference document from which they were derived.~~ The

requirement key words (i.e., REQUIRED, CONDITIONAL, etc) are defined elsewhere in thise UCR ~~2008~~. Failure to satisfy a requirement will result in a Category I, II, or III finding.

Finally, the ~~derived~~ requirements that follow do not include all of the administrative requirements (nontechnical) associated with policy and the STIGs. For instance, if someone is required to administratively document something (e.g. waiver, pilot request, etc.) as part of site accreditation, that requirement is not included. ~~The acronyms and appliances used for specifying the type of component are shown in~~ Table 5.4.6-1 shows the Acronyms and Appliances ~~, Acronyms and Appliances Specifying Type of Component~~which represent a specific UC APL product.

Table 5.4.6-1. Acronyms and Appliances Specifying Type of Component

ACRONYM	APPLIANCES
MFSS	Multifunction Softswitch
SS	Softswitch
LSC	Local Session Controller
MG	Media Gateway
EBC	Edge Boundary Controller
RSF	RTS Stateful Firewall
EI	End Instrument
AEI	AS-SIP End Instrument
LS	LAN Switch
R	Router
Smartphone_EI	Smartphone End Instrument
SBSS	Smartphone Backend Support System
FW	Data Firewall
VPN	Virtual Private Network concentrator and termination
IPS	Intrusion Detection/Prevention System

5.4.6.1.1 The [Alarm] Tag: Generation of Alarms

When the **[Alarm]** tag appears after a requirement's applicability statement (Required, Conditional, etc.), this indicates that the product must at a minimum support the capability to perform the following functions in addition to complying with the specified requirement:

1.) Generate an alarm to the NMS based on the alarmable actions identified in the requirement

2.) Record an entry in the product's system and audit logs indicating that the event occurred

This tag is intended to facilitate rapid identification all of those requirements that result in alarm conditions- by automated requirement management tools.

5.4.6.2 General and VVoIP Component Requirements

1. **[Required: MFSS, SS, LSC, MG, EBC, R, LS, EI, AEI, FW, IPS, VPN]** All Information Assurance and Information Assurance enabled Information Technology (IT) products shall be capable of being configured in accordance with all applicable DoD approved security configuration guidelines (i.e., STIGs).

   a. **[Required: MFSS, SS, LSC, MG, EBC, RSF]** VVoIP appliances shall be dedicated to VVoIP functions.

   b. **[Required: MFSS, SS, LSC, MG, EBC, RSF~~] VVoIP appliances~~, FW, IPS, VPN]** The appliance shall only have applications or routines that are necessary to support ~~VVoIP functions.~~its designated function.

      NOTE: The disabling or deletion of applications or routines via hardware or software mechanisms shall satisfy this requirement. For example, in the case of a VVoIP appliance, if an appliance by default is installed with a web browser and the web browser is not needed to support VVoIP, then the application shall be removed from the appliance. Another example is if a feature is part of the application, but is not needed in the DoD environment that feature shall be disabled via hardware or software mechanisms

      .

~~DoD~~

   c. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN]** Software patches shall only be installed if they originate from the system manufacturer and are applied in accordance with manufacturer's guidance.

      (1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN]** The product shall only accept automatic software updates if they are cryptographically signed by the software vendor.

      NOTE: It is assumed that manual updates will be validated by an authorized administrator before installation.

      NOTE: For JITC testing purposes, the vendor must provide a mock software update server to verify compliance with this requirement.

d. **[Required: FW, IPS, VPN]** The product shall be NIAP validated against existing current and approved protection profiles.

2. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS, FW, IPS, VPN]** If the product uses public domain software, unsupported software, or other software, it shall be covered under that system's warranty.

   NOTE: If a vendor covers in its warranty all software, regardless of its source, within their product then this requirement is met. An example of unsupported software is Windows NT, which is no longer supported by Microsoft and it is unlikely that a vendor would support this operating system as part of its system.

   a. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS, FW, IPS, VPN]** The products shall only use open source software if all licensing requirements are met.

      NOTE: It is anticipated that the Government will accept an LOC from a vendor as a means of satisfying this requirement. Open source software refers to software that is copyrighted and distributed under a license that provides everyone the right to use, modify, and redistribute the source code of the software. Open source licenses impose certain obligations on users who exercise these rights. Some examples include publishing a copyright notice and placing a disclaimer of warranty on distributed copies.

3. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN]** The product shall ~~not~~only use mobile code technologies (e.g., Java, JavaScript, VBScript, and ActiveX) ~~unless the mobile code technology is categorized and controlled~~ in accordance with the current DoD Mobile Code policy.

   NOTE: The policy specifying categories and risks associated with mobile code is defined in DoDI 8552.01, "Use of Mobile Code Technologies in DoD Information Systems", October 23, 2006.

4. **[Conditional: EI ~~and~~, AEI]** If the softphones are used in remote connectivity situations, the product shall be capable of supporting a VPN for VVoIP traffic from the PC to the Enclave VPN access router/node.

   NOTE: The data from the PC and VVoIP traffic from the PC softphone must be separated into the appropriate VLANs at the earliest point in the path.

5. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN]** The product shall be capable of being located in physically secure areas.

a. **[~~Required:~~ Conditional: MFSS, SS, LSC, MG, EBC, RSF~~]~~ ~~The~~, FW, IPS, VPN]** If the BIOS settings are configurable, the product shall be capable of enabling password protection of BIOS settings.

b. **[Required: MFSS, SS, LSC, MG, EBC, RSF, FW, IPS, VPN]** The product shall be capable of disabling the ability to boot from a removable media.

6. **[Conditional: EI, AEI]** If the product has a speakerphone, the system shall be capable of disabling the speakerphone microphone.

NOTE: Acceptable methods for meeting this requirement include physically disabling the speakerphone or disabling the speakerphone using a configurable software parameter.

7. **[Conditional: EI, AEI]** If the product is used in a sensitive area where NSS are employed and/or within environments where national security information (NSI) is stored, processed, or transmitted, then the system shall be certified and accredited in accordance with the Telephone Security Standard (TSG) 6, which is prepared by the National Telecommunications Security Working Group (NTSWG).

8. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN]** The product shall be capable of using a static IP address.

9. **[Required: MFSS, SS, LSC]** The product shall only connect to the PSTN or coalition networks using PRI and/or CAS.

NOTE: This precludes the exchange of SS7 or IP VVoIP signaling (and IP VVoIP media) information between the SBU voice (SS and LSC) and the PSTN and coalition networks.

10. ~~—~~**[Reserved]**

~~**[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI]** If the product uses a Microsoft Windows based operating system, the system shall support the installation and operation of the DoD mandated Host Based Security System (HBSS).~~

~~NOTE: The DoD currently has an enterprise wide license for McAfee's ePolicy Orchestrator (ePO) server, Host Intrusion Prevention System agent, and several associated agent applications. HBSS is being deployed by all C/C/S/As to all Windows based servers and workstations.~~

11. **[Required: MFSS, SS, LSC, EBC, MG, AEI, EI]** The system that assigns a port for the reception or transmission of SRTP and SRTCP based media as part of the session

establishment process shall have the capability to configure the range of ports used for media reception or transmission.

a. **[Required: MFSS, SS, LSC, EBC, MG, AEI, EI]** The system shall support the specification of port ranges in at least one of the following two ways:

- Using even numbers to specify the lower bound(s) and the upper bound(s) of the allowed range(s). In this case, the given range will include the SRTP port specified as the lower bound (inclusive), but the allowed range will not include the port specified for the upper bound (exclusive).

- Using an even number for the lower bound(s) and an odd number for the upper bound(s) of the allowed range(s). In this case, the given range will include both the SRTP port specified as the lower bound (inclusive) and the odd numbered SRTCP port specified as the upper bound (inclusive).

b. **[Required: MFSS, SS, LSC, EBC, MG, AEI, EI]** The default port range shall be from 16,384 to 32,764.

5.4.6.2.1 Authentication (Includes Authorization and Access Control)

5.4.6.2.1.1 Banners

1. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of having warning banners on all systems management ingress ports accessed by administrators or users as part of a human-to-machine interface for the purposes of network management. The banner shall function in the following manner:

   a. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** At the first point of entry, before the logon, the product shall have the capability to display a warning message that is at least 1,300 characters in length. The ability to display longer messages (20 rows by 80 characters) is desired (Objective).

      NOTE: The warning message may appear at the same time as the logon prompt or before the logon prompt.

   b. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** As part of delivered software, the product shall be capable of providing an appropriate default message that warns against unauthorized access or use.

      NOTE: The default message can be configured during the installation process.

c. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product banner shall be capable of being configured by authenticated and authorized personnel.

d. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of displaying the banner to the administrator or user before a login attempt to the system.

e. **[Required: MFSS, SS, LSC, MG, EBC, RSF]** The product shall be capable of requiring that the administrator or user acknowledges the banner after the user login but before accessing system processes.

(1) **[Required: MFSS, SS, LSC, EBC, RSF]** The product shall record the acknowledgement in the audit log in association with the administrator or user name.

NOTE: If the acknowledgement is an essential step in the successful login process, then it is sufficient to only log the completion of a successful login.

f. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of displaying the following information upon successful access to the product:

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The date and time of the administrator's or user's last successful access to the product.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The number of unsuccessful attempts by that user ID to gain access to the product (e.g., mistyped password) since the last successful access by that user ID.

g. **[Required: FW, IPS, VPN]** Prior to establishing a user authentication session, a security device shall display the latest approved DoD consent warning message to include verbiage that system usage may be monitored, recorded, and subject to audit.

5.4.6.2.1.2 System ~~and~~ User Names and Passwords

1. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS, FW, IPS, VPN]** Every communicating system entity (i.e., persons, processes, or remote systems) shall be identified by an entity identifier that is unique within the domain of the appliance or application ~~being~~to which the system entity is connected ~~to~~.

a. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall be capable of providing a primary access control method that is stronger than assigning passwords to specific actions (e.g., operations-related commands) although assigning passwords may be used to augment access control.

NOTE: If such a password is assigned, it loses its confidentiality because it has to be shared among all authorized users.

b. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall be capable of ensuring that all ~~users~~user and customer passwords are used in a secure manner.

NOTE: This requirement ~~is~~includes user/customer passwords to include passwords that are used for role-based authentication.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall be capable of automatically suppressing or blotting out the clear text representation of a password on the data entry device.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall ensure that passwords are safeguarded at the confidential level for sensitive but unclassified (SBU) systems.

NOTE: All components of a product will be at the same sensitivity level.

NOTE: The decision of how to properly safeguard the passwords is determined by the B/P/C/S DAA, but ~~as~~at a minimum these safeguards shall consist of encrypting the passwords during transit ~~or~~and while in storage using FIPS 140-2 commercial encryption.

(a) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall be capable of storing access passwords (user and administrator) in a one-way encrypted form.

(3) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall be capable of ensuring that passwords are not available in clear text to any user, including appropriate administrators. An appropriate administrator may be allowed to retrieve encrypted passwords. However, encrypted passwords shall not be available to any other user.

NOTE: It is recognized that ~~is~~it may not be realistic to make the encrypted password file unavailable to administrators. The administrator may be able to

view the file's content, but would not be able to decipher the encrypted passwords.

(4) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall be capable of providing a mechanism for a password to be user changeable. This mechanism shall require reauthentication of user identity (e.g. entry of the old password must occur when specifying the new password).

NOTE: This requirement applies to factory set, default, or standard user ID passwords.

(a) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall be capable of ensuring that a new user password differs from the previous password by at least four characters.

(b) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall be capable of having a password history to prevent password reuse. The default shall be configurable and shall be at least the past eight passwords or 180 days of password history.

(5) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** After a password is assigned to a human user, when that user establishes a session for the first time, the product shall be capable of prompting the user to change the password and deny the session if the user does not comply.

(6) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of enforcing a configurable password aging interval (i.e., a password is required to be changed after a specified interval).

NOTE: The exception to these requirements is found in the emergency access requirements in Section 5.4.6.2.1.7 "Authorization," paragraph 1 (l) and (m)).

~~NOTE: The exception to these requirements is found in the emergency access requirements in this UCR 2008 (Section 5.4.6, paragraph 1 (l) and (m)).~~

(a) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of defining a system-wide default password aging interval.

(b) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of setting the password aging interval on a "per-user ID basis."

i. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall notify the user a specified period of time before the password expiration.

ii. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall notify the user upon password expiration, but allow a specified additional number of subsequent logins within a specified time period before requiring a new password.

A. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The default for the number of subsequent logins shall not be greater than three.

B. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The default for the specified time period during which subsequent logins are allowed shall not be greater than 30 days.

iii. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall not hard code the notification mechanism for password expiration to allow for variation in variables such as "early warning period," "grace period," and subsequent login after password expiration.

(7) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** For a user updating a password, the product shall be capable of enforcing a configurable minimum period of waiting before an existing password can be updated (except for the first time update, which is required to be performed when the user logs in for the first time after being assigned a password).

NOTE: This requirement discourages password "flipping" and is related to the history requirements stated previously.

(a) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The default for the minimum waiting period shall be 24 hours without administrator intervention.

(8) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall be capable of ensuring that all user entered passwords meet the following complexity requirements (so that it ~~cannot be~~is not "easily guessable"):

(a) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of ensuring that the password consists of a mix of a minimum of nine characters using at least two characters from each of the four character sets (i.e., upper-case letters, lower-case letters, numbers, and special characters).

NOTE: Special characters are characters on a keyboard typically located above the numbers (i.e., !, @, #, etc.). NOTE: See the next requirement that is more stringent on certain users.

(b) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of ensuring that system security administrators, system administrators, and application administrator passwords consist of a mix of a minimum of 15 characters using at least two characters from each of the four character sets (i.e., upper-case letters, lower-case letters, numbers, and special characters).

NOTE: Special characters are characters on a keyboard typically located above the numbers (i.e., !, @, #, etc.).

(c) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, AEI, LS]** The product shall be capable of ensuring that the password does not contain, repeat, or reverse the associated user ID.

(d) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall be capable of ensuring that the password does not contain three of the same characters used consecutively.

(e) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall be capable of ensuring that a "null" password is not possible.

(f) **[Required: FW, IPS, VPN]** The security device shall be capable of setting and enforcing password syntax in accordance with current DoD Directives as defined in the latest JTF-GNO Communications Tasking Order 07-015.

(9) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** If passwords are generated by the product, the product passwords shall be capable of meeting the following requirements:

(a) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** Product supplied passwords shall be "reasonably" resistant to brute-force password guessing attacks, i.e., the total number of product - generated passwords shall be on the same order of magnitude as what a user could generate using the rules specified for user-entered passwords.

(b) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The generated sequence of passwords shall have the property of randomness, i.e., consecutive instances shall be uncorrelated, and the sequence shall not display periodicity.

(c) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** If the "alphabet" used by the password-generation algorithm consists of syllables rather than characters, the security of the password shall not depend on the secrecy of the alphabet.

(10) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall ensure that it does not prevent a user from choosing (e.g., unknowingly) a password that is already associated with another user ID (Otherwise, an existing password may be divulged).

(11) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall not permit passwords to be embedded in system defined access scripts or function keys.

(12) **[Conditional: MFSS, SS, LSC, MG]** If the product has the capability to display the "username of the last successful logon," then the product shall have the capability to enable and disable that feature.

(13) **[Conditional: MFSS, SS, LSC, MG]** If the product has the capability to display last logon information (e.g., successful/unsuccessful, date, and time details), the product shall provide the capability to disable and enable that feature.

(14) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** If PINs are used for passwords, the product shall have a configurable parameter for the PIN length and the range shall be between four (4) and twenty (20)

characters with a default of four (4).

NOTE: All password requirements defined in this section apply to PINs when used as passwords.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** If PINs are used for passwords, the product shall ensure that only numbers are allowed (i.e., no "#" or "*").

c. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** If PINs ~~(User IDs)~~ are used for user identification (~~versus~~e.g. the PIN is used as a user ID instead of as a password), the system shall be capable of ensuring that only one individual is permitted to use an assigned PIN.

NOTE: Since this can conflict with the preceding requirement, PINs (User IDs) must be assigned to users and they shall not be allowed to select their own PIN (User ID). This requirement only applies when a PIN is used for user identification without any other credential like a username or phone number.

(1) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** If PINs (User IDs) are used for user identification, the product shall have a configurable length between six (6) and twenty (20) characters and the default shall be 6.

(2) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** If PINs (User IDs) are used for user identification, the system shall only use numbers (i.e., no "#" or "*") when assigning the PIN (User ID).

NOTE: The uniqueness rules for the PIN (User ID) are the same as for any user ID as described in the following requirements.

d. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall be capable of ensuring that all authorized users and customers have unambiguous user IDs, such as MAC addresses or usernames, for identification purposes to support individual accountability, auditability, and access privilege.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall be capable of supporting the unambiguity of a user ID. This implies that the system shall prevent an appropriate administrator from creating (e.g., by mistake) a user ID that already exists.

e. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** At any given instance of time, the product shall be capable of internally maintaining the identity of all user IDs logged on at that time.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of associating a process that is invoked by a user or customer with the user ID of that user.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of associating a process that is invoked by another process, with the ID of the invoking process.

(3) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of associating an autonomous processes (i.e., processes running without user or customer invocation) with an identification code (e.g., "system ownership").

NOTE: An example of this would be a daemon on a UNIX workstation.

f. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** A product shall have the capability to ~~disable (as distinct from deleting)~~deny access to a user ID after a configurable specified time interval, if that user ID has never been used during that time interval.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** **[Alarm]** This capability shall be either an autonomous disabling of the user ID by the product along with an alarm/alert to notify the appropriate administrator, or an alarm/alert generated by the product for an appropriate administrator who then, depending on the policy, may disable or delete the user ID by using appropriate commands.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** A disabled or deleted login ID shall not be re-enabled by the user or another application user.

~~g.~~(3) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The ~~product shall have the capability to configure the~~ default ~~time interval~~value for ~~disabling a user ID that has not been used during that time interval. The default~~the configurable time interval shall be 90 days ~~In addition to disabling the user, the product shall be capable of sending an alert to the system security administrator~~.

g. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** If the system supports the capability to create temporary or emergency accounts, the system shall provide the capability to automatically terminate these accounts after a configurable time period.

h. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of verifying that a specified user (e.g., administrator) is only connected to the product a configurable number of times.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS] [Alarm]** An attempt for a specified user (e.g., administrator) to logon to the network a configurable number of times shall cause an alarm to be sent to the NMS unless an exception is granted per site policy.

Example: If a user should only be logged on once to the network, but the user attempts to logon while an active session for the same user is ongoing, this case could indicate a compromise of the user's credentials. Therefore, an alert must be sent to the appropriate administrators if configured.

i. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall be capable of allowing the system security administrator to configure the number of consecutive failed logins for a user before the login procedure shall exit and end the attempted session. The number of times shall be between two and five and the default shall be three.

NOTE: The exception to these requirements is found in the emergency access requirements (Section 5.4.6~~,~~.2.1.7 "Authorization," paragraph 1 (l) and (m)).

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall be capable of immediately notifying the user of a failed login (i.e., "Login Failed"). The error feedback generated by the system after the user authentication procedure shall provide no information other than "invalid," (i.e., it shall not reveal which part of the user-entered information [user ID and/or authenticator] is incorrect). Information such as "invalid user ID" or "invalid password" shall not be reported.

NOTE: It is acceptable to return a generic message such as "Account Locked" or "Account Disabled."

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall be capable of allowing a locked out user to be re-enabled by a

configurable timer or manually by an application security administrator, a system administrator, or a system security administrator.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** If a timer is utilized to re-enable a locked out user, the default for the lock-out duration shall be configurable and the default shall be 60 seconds when the threshold for incorrect user-entered information has been exceeded. (This is because longer delays can be used to temporarily disrupt the service by systematically locking out all input ports.)

(3) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS] [Alarm]** The product shall be capable of providing a mechanism to immediately notify (in real time) an appropriate administrator when the threshold for incorrect user-entered information is exceeded.

(4) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** When the threshold for incorrect user-entered information has been exceeded, the product shall not, as a default arrangement, suspend the associated user ID. (This is because suspension of user IDs can be used to systematically disable all user IDs.)

k. **[Required: FW, IPS, VPN] [Alarm]** For security devices, enforcement of session controls shall include system actions on unsuccessful log-ons (e.g., blacklisting of the terminal or user identifier).

(1) **[Required: FW, IPS, VPN]** For security devices, successive log-on attempts shall be controlled using one or more of the following:

- Access is denied after multiple unsuccessful logon attempts.
- The number of access attempts in a given period is limited.
- A time-delay control system is employed.

5.4.6.2.1.3 User Roles

1. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI]** The product shall be capable of having different types of user's roles.

NOTE: Section 5.4.5.2.1, User Roles, defines the different types of user roles. A vendor may rename the user roles as long as the requirements are met. The user roles are used for the purposes of originating VVoIP sessions and for network management functions.

a. **[Required: MFSS, SS, LSC]** The product shall be capable of having at least five types of user roles: A system security administrator, a system administrator, an application administrator, a privileged application user, and an application user.

b. **[Required: R, LS, EBC, RSF, MG]** The product shall be capable of having at least three types of user roles: A system security administrator, a system administrator, and an application administrator.

c. **[Required: EI, AEI]** The product shall be capable of supporting at least three types of user roles: a system administrator, a privileged application user, and an application user.

NOTE: The product demonstrates the ability to support a privileged application user by being able to dial precedence digits to signal the LSC the precedence of the session.

d. **[Required: EI, AEI]** The product shall be capable of setting the default user precedence VVoIP session origination capability as ROUTINE.

e. **[Required: MFSS, SS, LSC, MG, EI, AEI]** The product default user role shall be an application user.

f. **[Required: R, LS, EBC, RSF]** The product default user role shall be an application administrator.

g. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI]** The product shall be capable of working properly without Super User access privileges for any user application roles (system security administrator, a system administrator, an application administrator, and application user).

h. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI]** The product shall support appropriate system administrator functions as "separate" from other user functions.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI]** The security functions performed by an appropriate administrator shall be identified and documented.

(2) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI]** If the ability to enable or disable the administrator's account is an option of a

product, the products shall not require that the account be enabled or activated during normal operation.

(3) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of providing a mechanism for the appropriate administrator to perform the following functions:

(a) Display all users currently logged onto the product.

(b) Independently and selectively monitor (in real time) the actions of any one or more users, based on individual user identity.

(c) Monitor the activities of a specific terminal, port, or network address of the system in real time.

(d) Authorize users.

(e) Revoke users.

(f) Lock out and restore a specific system port or interface.

(g) Identify all resources accessible to any specific user along with the associated privileges required to access them. NOTE: Resources (i.e., files, applications, processes, etc.) should be denied to users unless specifically authorized access.

(h) Deny the creation of a user ID that is already in use.

(i) Disable or allow manual deletion of a user ID after a specific period of time during which the user ID has not been used.

(j) Reinstate a disabled user ID.

(k) Delete a disabled user ID.

(l) Create or modify a password associated with a user ID.

(m) Delete a user ID along with its password.

(n) Prevent the retrieval of a password in clear text.

(o) Define a password aging interval.

(p) Define the interval during which an expired password of a user shall be denied reusing a password.

(q) Define the events that may trigger an alarm, the levels of alarms, the type of notification, and the routing of the alarm.

(r) Define the duration of session lockout, which occurs when the threshold on the number of incorrect logins is exceeded.

(s) Specify a customized advisory warning banner that is displayed upon valid system entry.

(t) Define the duration of the time-out interval.

(u) Define the privilege of a user to access a resource.

(v) Define the privilege of an interface/port to be used to access a resource.

(w) Permit post-collection audit analysis tools for report generation.

(x) Permit the retrieval, copying, printing, or uploading of the security log.

(y) Deny the ability to modify or delete the security log.

(z) Provide a mechanism to specify the condition that would necessitate uploading the security log to avoid an overwrite in the buffer.

(aa) Provide a capability to validate the correct operation of the system.

(bb) Provide a capability to monitor the system resources and their availabilities.

(cc) Provide a capability to detect communication errors above an administrator defined threshold. The types of communications errors that must be detected include abnormally large numbers of received packets that fail decryption and/or fail to pass integrity checks (e.g. failed CRC or hash function computations).

i. **[Required: MFSS, SS, LSC, MG, EBC, RSF]** The product shall be capable of ensuring that a user's role or precedence ability has not changed during the execution

or exit from an application.

NOTE: The user shall not be able to use a control sequence mechanism, for example, shell escape to a SUPERUSER mode. Or, if the application fails, it must not leave the user in a different role with more privileges. The user must reauthenticate (relog-in) in order to assume a different role. If a system administrator has granted a user role limited root access (e.g., sudo for UNIX) it is part of that person's user role. This primary method to mitigate the threats associated with this requirement is to use industry best practices when developing the system.

j. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall only transmit passwords that are encrypted.

NOTE: The Backbone Transport Services STIG requires that router administrative passwords are hashed using MD5.

k. **[~~Required:~~ Conditional: MFSS, SS, LSC, MG, EBC, ~~RSF,~~ R, LS]** ~~The product~~If the system provides remote access, the system shall be capable of limiting user access based on a time of day interval (i.e., duty hours).

NOTE: Even during the times where remote access is restricted, local access is still permissible for emergency situations.

2. **[Required: FW, IPS, VPN]** The security device shall associate users with roles.

a. **[Required: FW, IPS, VPN]** The security device shall employ Role-Based Access Control (RBAC) in the local and remote administration of all device functions and operations.

b. **[Required: FW, IPS, VPN]** The security device shall associate all user security attributes with an authorized user.

c. **[Required: FW, IPS, VPN]** The security device shall allow and maintain the following list of security attributes for an authorized user:

(1) User identifier(s)
(2) Roles (e.g., System Administrator)
(3) Any security attributes related to a user identifier (e.g., associated certificate)

d. **[Required: FW, IPS, VPN]** The security device shall immediately enforce:

(1) Revocation of a user's role

(2) Revocation of a user's authority to use an authenticated proxy
(3) Changes to the information flow policy rule set when applied
(4) Disabling of service available to unauthenticated users

e. **[Required: FW, IPS, VPN]** The security device shall ensure all administrators can review the audit trail associated with their role.

f. **[Required: FW, IPS, VPN]** The security device shall ensure all roles can perform their administrative roles on the security device locally.

g. **[Required: FW, IPS, VPN]** The security device shall ensure all roles can perform their administrative roles on the security device remotely.

h. **[Required: FW, IPS, VPN]** The ability to perform the following functions shall be restricted to an Administrator defined or predefined (i.e., default) access control user role: to cryptography security data and/or the time/date method used for forming time stamps.

(1) **[Required: FW, IPS, VPN]** The ability to perform the following functions shall be restricted to the System Administrator role:

(a) Modify security functions.

(b) Enable/disable security alarm functions.

(c) Enable and/or disable Internet Control Message Protocol (ICMP) (in an IP-based network), or other appropriate network connectivity tool (for a non-IP-based network).

(d) Determine the administrator-specified period of time for any policy.

(e) Set the time/date used for timestamps.

(f) Query, modify, delete, and/or create the information flow policy rule set.

(g) Specify the limits on transport-layer connections.

(h) Revoke security attributes associated with the users, information flow policy rule set, and services available to unauthenticated users within the security device.

(2) **[Required: FW, IPS, VPN]** The ability to enable, disable, determine, and/or modify the functions of the Security Audit or the Security Audit Analysis shall be restricted to the AAdmin role.

(3) **[Required: FW, IPS, VPN]** The ability to perform the following functions shall be restricted to the CAdmin role:

(a) Enable and/or disable the cryptographic functions.
(b) Modify security functions.
(c) Modify the cryptographic security data.
(d) Enable/disable security alarm functions.

(4) **[Required: FW, IPS, VPN]** The security device shall restrict the ability to determine the administrator-specified network identifier

5.4.6.2.1.4 Ancillary Equipment

1. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI]** Products that use ancillary AAA and syslog services shall do so in a secure manner.

   NOTE: An external AAA service is a service that is extends beyond the boundary of the system whereas an onboard AAA service exists within the system boundary.

   a. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI]** Products that use external Authentication, Authorization, and Accounting (AAA) services provided by the Diameter Base Protocol shall do so in accordance with RFC 3588.

      ~~NOTE: An external AAA service is a service that is extends beyond the boundary of the system.~~

      (1) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI]** Systems that act as Diameter Agents shall be capable of being configured as Proxy Agents.

         (a) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI]** Systems that act as Proxy Agents shall maintain session state.

      (2) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI]** All Diameter implementations shall ignore answers received that do not match a known Hop-by-Hop Identifier field.

(3) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS, EI, AEI]** All Diameter implementations shall provide transport of its messages in accordance with the transport profile described in RFC 3539.

(4) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI]** Products that use the Extensible Authentication Protocol (EAP) within Diameter shall do so in accordance with RFC 4072.

b. **[~~Conditional:~~ Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI]** Products ~~that use external AAA services provided by~~shall support the capability to utilize the Remote Authentication Dial In User Service (RADIUS) ~~shall do so~~ in accordance with RFC 2865~~.~~ to provide AAA services.

NOTE: ~~The use of Diameter is preferred. Future~~Unlike previous UCR revisions where RADIUS was a Conditional requirement ~~revisions may mandate the use of Diameter~~, RADIUS is now a capability that is required when supporting AAA services.

(1) **[~~Conditional:~~ Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI]** Products that use the EAP within RADIUS shall do so in accordance with RFC 3579.

(2) **[~~Conditional:~~ Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI]** If the products support RADIUS based accounting, the system shall do so in accordance with RFC 2866.

(3) **[~~Conditional:~~ Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI]** If the product supports RADIUS, it shall support the use of IPSec and/or TLS using non-null transforms as defined in the confidentiality section of this UCR ~~2008~~ (Section 5.4.6, Requirements).

(4) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI]** If the product supports RADIUS and IPSec, it shall support the use of IKE for key management as defined in the confidentiality section of this UCR ~~2008~~ (Section 5.4.6, Requirements).

c. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI]** Products that use external AAA services provided by the Terminal Access Controller Access Control System (TACACS+) shall do so in accordance with the TACACS+ Protocol Specification 1.78 (or later).

NOTE: The intent is to use the most current TACACS+ specification.

~~NOTE: The intent is to use the most current specification. The use of Diameter is preferred. Future requirement revisions may mandate the use of Diameter.~~

(1) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI]** If the product supports TACACS+, it shall support the use of IPSec and/or TLS using non-null transforms as defined in the confidentiality section of this UCR (Section 5.4.6, Requirements).

(2) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI]** If the product support TACACS+ and IPSec, it shall support the use of IKE for key management as defined in the confidentiality section of this UCR (Section 5.4.6, Requirements).

d. **[Conditional: EI, AEI]** Products that use external address assignment services provided by the DHCP shall do so in accordance with RFC 2131.

NOTE: An external address assignment service is a service that extends beyond the boundary of the system.

(1) **[Conditional: EI, AEI]** Products that act as DHCP clients upon receipt of a new IP address shall probe (e.g., with ARP) the network with the newly received address to ensure the address is not already in use.

NOTE: The actions to take if a duplicate address is detected are found in RFC 2131.

(2) **[Conditional: EI, AEI]** Products that act as DHCP clients upon receipt of a new IP address shall broadcast an ARP reply to announce the client's new IP address and clear outdated ARP cache entries in hosts on the client's subnet.

e. **[Conditional: R, LS, EI, AEI]** Products that use external AAA services provided by port based network access control mechanisms shall do so in accordance with IEEE 802.1X-2004 in combination with a secure EAP type (EAP-TLS, EAP-TTLS, or PEAP).

(1) **[Conditional: R, LS, EI, AEI]** Products that use external EAP services provided by EAP shall do so in accordance with RFC 3748 and its RFC extensions.

(a) **[Conditional: R, LS, EI, AEI]** Products that support EAP as a minimum shall support authentication using shared secrets.

NOTE: RFC 3748 requires that systems support Identity, Notification, Nak, and MD-5 Challenge Request/Response exchanges.

f. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** Products that use external syslog services shall do so in accordance with RFC 3164~~.~~ and **[Required UCR 2012]** RFC 5424.

NOTE: Even in UCR 2012, support for RFC 3164 formatted syslog messages would still be required for backwards compatibility.

~~NOTE: It is understood that an Internet Draft is written that will deprecate RFC 3164, but that draft is new and it is unknown whether it will be approved.~~

(1) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** Products that support syslog over UDP in accordance with RFC 3164 shall use UDP port 514 for the source port of the sender when using UDP for transport.

(2) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** ~~Products that support~~ If the product supports syslog, the product shall support the capability to transmit messages in the format defined by RFC 3164.

(3) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** ~~Products that support~~ If the product supports syslog, the product shall support the capability to generate syslog messages which have all the parts of the syslog packet as described in Section 4.1 of RFC 3164.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** If the originally formed message has a TIMESTAMP in the HEADER part, then it shall be the local time of the device within its time zone.

(b) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** If the originally formed message has a HOSTNAME field, then it shall contain the hostname as it knows itself. If it does not have a hostname, then it shall contain its own IP address.

(c) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** If the originally formed message has a TAG value, then it shall be the name of the program or process that generated the message.

(4) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** If products use TCP for the delivery of syslog events, then the system shall do so in

accordance with the RAW profile defined in RFC 3195.

~~NOTE: It is understood that an Internet Draft is written that will deprecate RFC 3195, but that draft is new and it is unknown whether it will be approved~~

NOTE: At the time of this document's writing, it is believed that IETF "draft-gerhards-syslog-plain-tcp" will deprecate RFC 3195. When approved, it is expected that this standard will be mandated in the UCR for TCP Syslog implementations.

NOTE: The capability to provide reliable delivery for syslog events is expected to be mandated as hard requirement in future UCR versions.

(5) **[Required UCR 2012: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** If the product supports the transmission of syslog messages over UDP, it shall support the capability to do so in accordance with RFC 5424 and RFC 5426 "The Transmission of Syslog Messages over UDP."

(6) **[Required UCR 2012: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** If the product supports the transmission of syslog messages over TLS, it shall support the capability to do so in accordance with RFC 5424 and RFC 5425 "The Transport Layer Security (TLS) Transport Mapping for Syslog" (including any errata that may exist).

(a) **[Required UCR 2012: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** If the product supports the transmission of syslog messages over TLS, the TLS profile used to support RFC 5425 shall confirm to all of the applicable TLS requirements in this UCR.

(b) **[Required UCR 2012: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** If the product supports the transmission of syslog messages over TLS, the product shall support the use of X.509v3 certificates issued from a DoD approved PKI in order to support mutual authentication with the syslog server.

(7) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** If the product supports delivery of sylsog events, the product shall support the capability to:

a. Detect network connectivity errors
b. Provide a mechanism to buffer a configurable number of syslog events
c. Deliver any buffered events once network connectivity is restored

NOTE: This requirement applies not only to scenarios where reliable delivery allows for detection of lost messages, but also to connectionless transports like UDP where OSI layer 1, 2, or 3 connection errors prevent successful delivery of messages onto the network.

2. **[Required: FW, IPS, VPN]** The security device shall be able to use at least one external authentication method (e.g., RADIUS, TACACS+, and/or LDAP).

3. **[Required: EBC]** The EBC shall either support an onboard VVoIP IDS/IPS capability that can monitor all VVoIP signaling and media traffic in decrypted form, or support the capability to present all signaling and bearer traffic to an external VVoIP IDS/IPS in a secure manner.

   a. **[Required: EBC] [Alarm]** The VVoIP IDS/IPS threat detection capabilities shall be in accordance with the VVoIP IDS/IPS functional requirements specified in Section 5.8 of this UCR. The product shall alarm to the NMS when these threats are identified.

   b. **[Conditional: EBC]** If the EBC provides the capability to transmit decrypted media and signaling to an external VVoIP IDS/IPS platform, the EBC shall at a minimum provide FIPS-compliant confidentiality and integrity for this information in an manner that conforms to the crytographic profiles specified for TLS and IPSec in this UCR.

   c. **[Conditional: EBC]** If the EBC provides the capability to transmit decrypted VVoIP media and signaling to an external IDS/IPS platform, this interface shall use publicly accessible specifications and standards.

      NOTE: The intent of this requirement is to ensure that third party IDS/IPS vendors have the information necessary to create an interface that can accept and process the received VVoIP information.

5.4.6.2.1.5 Authentication Practices

1. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI]** The product shall be capable of authenticating users and appliances.

   a. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall only allow authenticated users and appliances to access the system.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall ensure that authentication credentials are not transmitted in the "clear" (i.e., credentials are encrypted end-to-end).

NOTE: The PKI certificate does not fall under this requirement due to the nature of the public key authentication model.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN]** The product shall be capable of ensuring that system access points that provide remote login facility also provide authentication services that are capable of utilizing authentication mechanisms that are stronger than usernames and passwords (i.e., using two-factor authentication [strong authentication~~]).~~] and using an I&A technique that is resistant to replay attacks).

(a) **[Required: FW, IPS, VPN]** The security device shall require user identification and authentication via one of the following specified methods before enabling user access to itself or any device under its control:

a. Local access authentication mechanism.

b. Remote access two-factor, authentication mechanism implementing the DoD Public Key Infrastructure (PKI) authentication (defined in detail in Section 5.4, Information Assurance Requirements), either internal to security device or via an external AAA service such as RADIUS or TACACS+.

(b) **[Required: FW, IPS, VPN]** The security device shall provide a local authentication mechanism to perform user authentication.

(3) **[Required: LSC]** The product shall be capable of authenticating the EI using TLS (or its equivalent) (Threshold) ~~and/or~~ with PKI certificates~~.~~ issued from a DoD approved PKI.

NOTE: This assumes the EI is served directly by the appliance.

(4) **[Required: LSC]** The product shall be capable of authenticating the AEI using TLS with PKI certificates issued from a DoD approved PKI.

(5) **[Required: EI]** The product shall be capable of authenticating the LSC using TLS (or its equivalent) (Threshold) ~~and/or~~ with PKI certificates issued from a DoD approved PKI.

(6) **[Required: AEI]** The product shall be capable of authenticating the LSC using TLS with PKI certificates issued from a DoD approved PKI.

b. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI]** The product shall be capable of authenticating an appliance using the ~~DoD PKI.~~

~~NOTE: The EI authentication is excluded from this requirement in FY 2008.~~certificates issued by a DoD approved PKI.

(1) **[Conditional: ~~-~~LSC, SS, EBC, RSF, MFSS, EI, AEI]** If the product is PKE, then the system shall use ~~the DoD~~ PKI certificates issued from a DoD approved PKI with the associated public key in the TLS certificate message for authenticating appliance when using AS~~-~~-SIP.

NOTE: Some options considered to meet this requirement include the use of ~~OSC~~OCSP responders and certificate trust lists as discussed in Section 5.4~~.5.2.7, paragraph 1(g).~~ of this UCR.

(2) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF]** If the product supports web browsers and web servers, the system shall be capable of using ~~DoD PKI~~ certificates issued by a DoD approved PKI with the associated public key in the TLS certificate message for authenticating users.

c. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall be capable of ensuring that user authentication for logging in, logging, and auditing of an appliance shall be at least as strong as a user ID and the appropriate password/PIN (user ID) entered over a previously established trusted path.

NOTE: The previously established trusted path ensures that the password is not transmitted in the clear. It is acceptable for systems to use RADIUS, TACACS+, or Diameter for AAA services.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** If a CAC or other PKI token approved by the DoD PKI PMO (e.g. PIV) is used for authentication purposes, the ~~CAC~~ user's credentials from the CAC or token shall be passed by the authentication mechanism (i.e., local authentication, RADIUS, DIAMETER, TACACS+, etc.) to the ~~product~~ product's management and configuration applications for the purposes of providing role-based access control.

NOTE: For example, this means that the product should not have to require a

second authentication, such as a username and password, to occur for ~~EMS functions.~~ authorization purposes after the CAC or other approved token-based authentication has successfully completed.

d. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall not support ways to bypass the deployed authentication mechanism.

e. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall perform the entire user authentication procedure even if the user ID that is entered is not valid.

NOTE: The notification requirements associated with a failed login are covered in ~~the~~ other requirements in this section of the UCR ~~2008~~.

f. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall protect (i.e., encrypt) all internal storage of authentication data to ensure confidentiality.

NOTE: This requirement is not meant to preserve session keys during a power cycle. It is primarily meant to ensure that an intruder that gains access to the system is not able to view the authentication information in clear text.

g. **[Required: EI, AEI]** The product shall be capable of allowing users to place ROUTINE precedence and emergency calls without authenticating.

h. **[Required: EI, AEI]** The product shall only allow authenticated users to access the product for services above the ROUTINE precedence.

(1) **[Conditional: LSC, EI, AEI]** If the product uses SIP, the system shall use digest authentication as specified in RFC 3261 and/or with PKI certificates for authenticating user credentials to the LSC via the EI or the AEI.

NOTE: The LSC is responsible for the authentication decisions. The method for authenticating a user with their PKI certificate is a vendor decision due to the immaturity of the current standards. Vendors may choose to implement user authentication using PKI certificates as described in RFC 3261 or as described in RFC 3893.

(2) **[Required: LSC, EI, AEI]** The user authentication mechanism shall be software enabled or disabled.

NOTE: In certain deployments, the user does not have the time to input

authentication credentials and the EI or AEI is located in a secure environment where credentials are not necessary due to the mission. By default this capability will be disabled to allow users to place calls without authenticating.

(a) **[Required: EI ~~and~~, AEI, (Softphone)]** If the product is a softphone, the product shall provide user authentication by presenting the ~~CAC~~ user credentials ~~of~~extracted from the ~~user~~CAC or other DoD PKI PMO approved PKI token to the LSC.

i. **[Required: EI, AEI]** The product shall only allow an authenticated system administrator to perform configuration functions.

NOTE: This requirement is focused on network and LSC configuration items and is not meant to preclude users from personalizing the phone through configuration items like volume control (to include mute), speakerphone enable/disable (if originally enabled by the system administrator), headset enable/disable, LCD contrast, voice mail features, speed dial and call forwarding features.

i. **[Required: EI, AEI]** The product shall not display configuration information without proper authentication.

NOTE: The minimum requirement for authentication is defined ~~UCR 2008,~~this section of the UCR, Section 5.4.6.2.1.5, Authentication Practices~~, paragraph 1.c~~.

j. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of ensuring that all ports on a system that support operations related command inputs (e.g., SNMP SET commands) exercise strong authentication mechanisms for access control.

k. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of ensuring that all appliances that support connection-oriented communications also support mutual authentication between the requestor and the provider.

NOTE: A connection-oriented communication is a session between two VVoIP appliances where the Transport Layer Protocol sends acknowledgments to the sender regarding incoming data. This type of session usually provides for retransmission of corrupted or lost data.

l. **[Required: EI, AEI]** The product shall properly operate when auto-registration is disabled.

NOTE: Auto-registration is typically used during initial installation of large numbers of EIs. It involves the automatic registration of EIs to the LSC, automatic assignment of IP assignment of IP addresses and user IDs, and automatic download of application files. Typically, auto-registration is disabled after installation and manual changes are made.

m. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The default authentication mechanism for SNMPv3 shall be HMAC-SHA-96. Therefore, the product will present HMAC-SHA-96 on the appropriate SNMPv3 configuration interface as the default authentication mechanism.

n. **[Required: FW, IPS, VPN]** Identification and Authentication management mechanisms shall include, in the case of communication between two or more systems (e.g., client server architecture), bidirectional authentication between the two systems.

5.4.6.2.1.6 Public Key Infrastructure

1. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ,~~ EI]** The product shall be capable of meeting the DoD Public Key Enablement (PKE) requirements for PKI based authentication.

NOTE: The requirement for an EI to be PKE ~~is~~ was conditional for ~~this iteration of the~~ UCR 2008 Change 1, but ~~will be~~is now required in ~~the~~ UCR 2010. ~~The condition for this iteration of the UCR is that if the EI is PKE, it shall meet the PKE requirements.~~

a. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ,~~ EI]** The product shall be capable of generating asymmetric (public and private) key pairs and symmetric keys.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ,~~ EI]** The product shall be capable of generating asymmetric keys whose length is at least ~~1024~~2048 for RSA.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ,~~ EI]** The product shall be capable of generating symmetric keys whose length is at least 128 bits~~.~~ or **[Required UCR 2012]** 256 bits.

(a) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~– Conditional: ,~~ EI]** The product shall be capable of distributing keys used for symmetric encryption out-of-band or by secure cryptographic processes that comply with in FIPS 140-2.

(3) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~– Conditional: ,~~ EI, FW, IPS, VPN]** The product shall be capable of generating keys using a random source algorithm that meets the requirements of ~~FIPS 186~~:

a. FIPS 186 if the product's randomizer is approved by NIST before and including 2010
b. NIST SP 800-90 if the product's randomizer is approved by NIST after 2010

NOTE: At the time of this document's writing, draft NIST SP 800-131 fully deprecates FIPS 186 randomizers after the year 2015.

b. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~– Conditional: ,~~ EI]** The product shall be capable of storing key pairs and their related certificates.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~– Conditional: ,~~ EI]** The product shall be capable of storing certificates for a subscriber.

NOTE: A subscriber may be itself, another appliance, or a user of the product. The certificates may have the same public key and may be associated with different issuers, different uses, or different validity periods. The certificates are stored on the appliance for a variety of reasons including for historical purposes. This requirement is for local authentication of the user and is not meant to obtain the private key of the subscriber.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~– Conditional: ,~~ EI]** The product shall be capable of protecting the private key from compromise or loss.

NOTE: The ~~requirement may be satisfied by meeting~~product must minimally meet the requirements of FIPS 140-2 for protecting keys and also conform to any requirements that are more stringent which are specified in this UCR.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI]** If the certificate shall be used for non-repudiation purposes, the product shall be capable of ensuring that all copies of private keys generated for actual or possible non-repudiation purposes are under the owning

entity's sole control.

NOTE: A subsequent requirement mandates that the system is capable of using the certificate for non-repudiation by setting the key usage extension for non-repudiation. An example of a need for non-repudiation is to verify that a user made a malicious configuration change on the platform.

(b) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI]** The product shall be capable of meeting the requirements for level 1 of FIPS 140-2 ~~in FIPS Mode (i.e., approved for federal Government use as opposed to commercial use).~~and operate in a FIPS approved mode as defined in FIPS 140-2.

NOTE: Where the requirements listed are more secure than FIPS 140-2, UCR 2008 requirements supersede FIPS 140-2.

(c) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI]** If the product performs operations with the unencrypted key in software, the system shall be capable of encrypting or destroying the key as soon as the operation is complete.

(d) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI]** If passwords are used to protect private keys, the product shall be capable of ensuring that the password ~~is selected from a space of at least 2^{56} possible passwords unless there is a means to detect and protect against deliberate attempts to search for passwords.~~meets at a minimum the requirements in this UCR for password complexity (size, character type, and diversity).

NOTE: This requirement is meant to prevent a malicious user from using password guessing to gain access to the private keys. ~~The requirement may be met by meeting the requirement defined in requirements Section 5.4.5.2, Authentication. The requirement applies only if passwords are used to protect private keys.~~ The requirement, by itself, does not mandate passwords. In accordance with the Application Security and Development STIG, private keys must be accessible only to administrative users.

(e) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ~~,~~ EI]** The product shall operate with DoD approved trust points~~.~~ (e.g. public keys and the associated certificates the relying

party deems as reliable and trustworthy, typically Root Certificate Authorities).

NOTE: Trust points are further defined in ~~UCR 2008,~~ Appendix A of this UCR, Definitions, Abbreviations and Acronyms, and References.

i. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ,~~ EI]** The product shall ~~obtain the status of~~authenticate individual certificates ~~from~~up to a ~~DoD~~ trust point.

ii. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI]** If ~~the~~a trust point is not established, the product shall ~~obtain the status of~~authenticate individual certificates from the issuer specified on the individual certificate ~~or from~~up to the root certificate authority (CA).

c. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ,~~ EI]** The product shall be capable of protecting certificates that are trust points.

NOTE: Methods used to protect trust points include restricting access to and use of this capability to designated individuals.

d. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ,~~ EI]** The product shall be capable of supporting end entity server and device certificates in accordance with methods described in the DoD PKI Functional Interface Specification (June 2007).

~~(1) [Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI – Conditional: EI] The product shall be capable of using HTTPS to request and obtain certificates for the subscriber.~~

~~(a) [Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI – Conditional: EI] If the product uses HTTPS to request and obtain certificates, then the product shall be capable of encrypting and decrypting using the Triple Data Encryption Algorithm (TDEA).~~

e. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ,~~ EI]** The product shall be capable of importing key pairs, related certificates, and certificate revocation information.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ,~~ EI]** The product shall be capable of using the LDAPv3~~ or,~~ HTTP, or HTTPS as appropriate when communicating with the DoD PKI.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ,~~ EI]** The product shall ~~be capable~~support all of ~~accepting needed old certificates (i.e., certificates that have expired or been revoked) and CRLs (Certificate Revocation List) (i.e., CRLs whose next update is after~~ the ~~current date) from~~applicable requirements in the latest DoD PKE Application Requirements specification published by the DoD PKI ~~archive using HTTPS~~PMO.

NOTE: At the time of this document's writing, it is envisioned that a new version of the DoD PKE Application specification originally published in 2000 will soon be released.

(3) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI]** The product shall be capable of requesting and accepting information regarding the status of certificates using CRLs or the ~~On-line~~Online Certificate Status ~~Check~~ Protocol (OCSP) as defined in RFC 2560 and in the DoD PKI Functional Interface Specification dated June 2007.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI]** If CRLs are used, the product shall be capable of using either the date and time specified in the next update field in the CRL or using a configurable parameter to define the period associated with updating the CRLs.

~~i. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI]** If a configurable parameter is used as the basis for updating the CRLs, then a default value for the period associated with updating the CRLs shall be 24 hours.~~

(b) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI]** If CRLs are used, the product shall be capable of obtaining the CRL from the CRL Distribution Point (CDP) extension of the certificate in question. The product shall be able to process HTTP pointers in the CDP field whereas the ability to process HTTPS and LDAP pointers is objective.

(c) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI]** If OSCP is used, the product shall support the capability to utilize the Delegated Trust Model (DTM), whereby the OCSP responder's

certificate is signed by a DoD approved PKI CA, in accordance with DoD PKI PMI guidance.

NOTE: The OCSP responder's DTM certificate is appended to every OCSP response sent from the DoD PKI OCSP responders. Products should expect this certificate to change regularly.

(d) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI]** If OCSP is used, the OCSP Responder shall be contacted based on the following information:

1) The OCSP Responder pre-configured in the application or toolkit; and

2) The OCSP Responder location identified in the OCSP field of the AIA (Authority Information Access) extension of the certificate in question.

3) If both of the above are available: The product shall be configurable to provide preference for one over the other.

4) The product should (not shall) be configurable to provide preferences or a pre-configured OCSP Responder based on the Issuer DN.

(4) **[Required: EI]** The EI shall support a mechanism for verifying the status of an LSC certificate using a Certificate Trust List (CTL~~) or via the OSCP.~~), CRLs, an online status check (OSCP in the case of the DoD PKI).

NOTE: It is understood that the system administrator must ensure that the CTL is current to ensure that the status is accurate.

NOTE: When implemented the CRL and OSCP implementation must conform to the CRL and OSCP requirements specified previously and later in this section.

(5) **[~~Conditional:~~ Required: LSC]** ~~If the EI is DoD PKE, the~~The LSC shall verify the status of an EI certificate using the Certificate Trust List (CTL~~or~~), CRLs, an ~~OSC.~~online status check (OSCP in the case of the DoD PKI).

NOTE: It is understood that the system administrator must ensure that the CTL is current to ensure that the status is accurate.

NOTE: When implemented the CRL and OCSP implementation must conform to the CRL and OSCP requirements specified previously and later in this section.

f. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ~~, EI]** The product shall be capable of performing public key operations necessary to verify signatures on DoD PKI signed objects (i.e. certificates, CRLs, and ~~OSC~~OCSP responder responses).

(1) **[Required: ~~-~~MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ~~, EI]** The product shall be capable of producing SHA digests of messages to support verification of DoD PKI signed objects.

(a) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI]** The product shall support the capability to verify certificates, CRLs, OCSP responses, or any other signed data produced by a DoD approved PKI using RSA in conjunction with the SHA-256 algorithm.

NOTE: During the migration to SHA-256, certificate chains may contain a mix of certificates signed using either SHA-1 or SHA-256 within the same chain.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI]** The product shall reject all new sessions associated with a revoked certificate.

(3) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R]** The product shall log when a session is rejected due to a revoked certificate.

g. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ~~, EI]** The product shall be capable of supporting the development of a certificate path and be able to process the path.

NOTE: The path development process produces a sequence of certificates that connect a given end-entity certificate to a trust point. The process terminates when either the path tracks from a trust point to an end entity or a problem occurs that prohibits validation of the path.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ~~, EI]** The product shall be capable of verifying certificate signatures using the certificate issuer's public key.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ,~~ EI]** The product shall be capable of ensuring that the effective date falls within the certificate's validity period.

NOTE: The effective date is the date when the transaction was initiated. Normally, the effective date should be considered the current date unless reliable evidence exists to establish an earlier effective date.

(3) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ,~~ EI]** The path process shall fail when a problem that prohibits the validation of a path to occur.

(4) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ,~~ EI]** The product shall be capable of ensuring the validity of certificates through a status check.

NOTE: The status check is done at the time the certificate is presented to the appliance. Status checking involves checking the status of certificates in the path to ensure that none are revoked.

(a) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ,~~ EI]** The product shall be capable of verifying the signature of ~~-~~the CRL or the ~~OSC~~online status check response~~.~~ (for the DoD PKI, this will be an OCSP responder response message).

i. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI]** ~~If~~**[Alarm]** During VVoIP session establishment, if the product uses ~~the OSC~~an online status check to validate a certificate and the product cannot contact the online status check responder (OSCR) (in the case of the DoD PKI, this will be an RFC 2560 OCSP responder) and backup OSCRs, the product will ~~continue the process,~~establish the VVoIP session (e.g. shall not terminate the session), but will log the event and send an alarm to the NMS.

NOTE: This requirement applies only to the establishment of VVoIP sessions. This requirement is not applicable to scenarios related to non-VVoIP-session related functions such as logging in to administrative interfaces. The intent of this requirement is to prevent phone calls from being denied due to connectivity issues with the OCSP responder.

ii. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI]** **[Alarm]** During VVoIP session establishment, if the product uses CRLs to validate a certificate and the product cannot reach the CRL Distribution Point (CDP) or any backup CDPs, the product will continue the process (e.g. shall not terminate the session), but will log the event and send an alarm to the NMS.

NOTE: This requirement applies only to the establishment of VVoIP sessions (see the note on the preceding requirement).

(b) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI]** The product shall be capable of verifying that the CRL has not expired (even if the target certificate has not expired) or shall be capable of verifying that the ~~OSC~~online status check response (in the case of the DoD PKI, this will be an OCSP response) indicates the certificate is valid.

NOTE: The intent of this requirement is to ensure that the ~~OSCR~~online status check response or CRL is valid before completing the status check.

(c) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ~~, EI]** The product shall be capable of searching the list of revoked certificates to determine that the target certificate is not included or the revocation date is after the effective date.

(d) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ~~, EI]** The product shall be capable of rejecting expired certificates.

NOTE: An example of this case would exist if a certificate's effective date is reliable, but the certificate has since expired.

(e) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI]** The product shall log an event if the certificate is rejected due to a status check.

(5) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ~~, EI]** The product shall be capable of ensuring that the intended use of the certificate is consistent with the DoD PKI extensions.

(6) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ,~~ EI]** The product shall be capable of ensuring that the key usage extension in the end entity certificate is properly set.

(a) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ,~~ EI]** The product shall be capable of ensuring that the digital signature bit is set for authentication uses.

(b) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ,~~ EI]** The product shall be capable of ensuring that the non-repudiation bit is set for non-repudiation uses.

(c) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI~~ – Conditional: ,~~ EI]** The product shall be capable of ensuring that the DoD PKI fields are populated in accordance with the DoD PKI Functional Interface Specification dated June 2007.

h. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI]** The system shall periodically examine all of the certificates and trust chains associated with ongoing, long-lived, sessions. The system shall terminate any ongoing sessions on the basis of updated revocation/trust information if it is determined that the corresponding certificates have been revoked, are no longer trusted, or are expired.

NOTE: The system must not terminate VVoIP sessions simply because of a failure to retrieve the latest CRL or perform an online status check (see Section 5.4.6.2.1.6 Paragraph 1.g.4.a.i and 1.g.4.a.ii)

(1) **[Conditional: MFSS, SS, LSC, MG, EBC, R, AEI, EI]** If the system supports manual loading of a CRL or certificate trust lists configured by an administrator, the system shall check all ongoing sessions as soon as updates to the internally stored CRL or trust lists occur.

(2) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI]** If the system supports automated retrieval of a CRL from a CRL distribution point (CDP), the system shall immediately check the certificates and trust chains associated with all ongoing sessions against the newly retrieved CRL.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI]** If the system supports automated retrieval of a CRL from a CRL distribution point, by default, devices shall retrieve the latest CRL every 24 hours.

(b) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI]** If the system supports automated retrieval of a CRL from a CRL distribution point, the system shall support the ability to configure the interval in which the CRL is periodically retrieved.

(3) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI]** If the system supports queries against an online status check responder (an OCSP responder in the case of the DoD PKI), the system shall periodically query the responder to determine if the certificates corresponding to any ongoing sessions have been revoked.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI]** If the system supports queries against an online status check responder (an OCSP responder in the case of the DoD PKI), by default, for each session, the device shall query the online status check responder every 24 hours for as long as the session remains active.

(b) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI]** If the system supports queries against an online status check responder (an OCSP responder in the case of the DoD PKI), the system shall support the ability to configure the interval at which the system periodically queries the online status check responder.

i. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI] [Alarm]** The system shall be capable of sending an alert when installed certificates corresponding to trust chains, OCSP responder certificates, or any other certificates installed on the device that cannot be renewed in an automated manner, are nearing expiration.

NOTE: Since EIs and AEIs are not expected to have direct access to the NMS, the LSC, MFSS, or SS is expected to generate this alert to the NMS on behalf of any subtended EIs or AEIs.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI] [Alarm]** By default, the system shall be capable of sending this alert 60 days prior to the expiration of the installed credentials which cannot be automatically renewed. This alert should be periodically repeated on a weekly or bi-weekly basis by default.

j. **[Required: MFSS, SS, LSC, MG, EBC, AEI, EI]** The product shall verify that the identity claimed in an X.509v3 certificate, used to establish an authenticated and secure channel, correctly maps to the identity claimed in signaling messages transmitted within the same secure channel.

NOTE: In the case of AS-SIP, an example would be ensuring that the previous hop specified by the domain parameter of a SIP URI in an AS-SIP Route header matches the identity specified in the Subject Common Name field of the X.509v3 certificate received during TLS session establishment.

NOTE: At this time the identity claimed in an X.509v3 certificate may be a FQDN, IPv4, or IPv6 address.

(1) **[Required: MFSS, SS, LSC, MG, EBC] [Alarm]** The product shall support the capability to generate and transmit an alarm to the NMS when it detects a mismatch between the identity claimed in an X.509v3 certificate used to establish a secure channel at a lower layer, and the identity claimed in messages within the established secure session. Furthermore, the product shall deny the operation requested by the message containing the mismatched identity.

NOTE: Examples include cases where a device attempts to use a phone number not assigned to the identity claimed in the X.509v3 certificate presented by the device. Another example includes cases where the domain in the SIP URI of a Route header unexpectedly does not match the identity in the X.509v3 certificate.

(2) **[Required: MFSS, SS, LSC, MG, EBC, EI, AEI]** The product shall support the capability to examine the identity claimed by the X.509v3 Subject Common Name field and compare it to the identity claimed within signaling messages regardless of whether the claimed identity contains an FQDN, IPv4 address, or IPv6 address.

(3) **[Required UCR 2012: MFSS, SS, LSC, MG, EBC, AEI, EI]** The product shall support the capability to examine all of the identities presented in the Subject Alternative Name and the Subject fields of the X.509v3 ceritficate to determine if any of these fields contain a FQDN, IPv4 address, IPv6 address, or SIP URI that corresponds to the appropriate identity contained in signaling messages.

(4) **[Required: MFSS, SS, LSC, MG, EBC, AEI – Conditional: EI]** The product shall adhere to the requirements in RFC 5922 Section 7.2 "Comparing SIP Identities" when comparing the domains extracted from X.509v3 certificates with SIP identities contained in signaling messages.

NOTE: The condition for EIs is the use of SIP or AS-SIP.

(5) **[Conditional: MFSS, SS, LSC, MG, EBC, AEI, EI]** If the product does not support DNS, the product shall support the capability to statically map the FQDNs contained in X.509v3 certificates to IP addresses via a configurable lookup table.

(a) **[Objective: MFSS, SS, LSC, MG, EBC, AEI, EI]** The product shall support the capability to use DNS to map the FQDNs contained in X.509v3 certificates into IPv4 or IPv6 addresses.

5.4.6.2.1.7 Authorization

1. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI, LS]** The product shall be capable of providing authorization for services accessed on the system.

   a. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, LS]** The product shall be capable of denying system access to any user unless identified with a user ID and authenticated. Only authorized users shall be allowed system access. This holds for all users (i.e., persons, processes, or remote systems).

      NOTE: This requirement applies to multiple access types to include remote login, telephony services, and direct system access. However, 911 and emergency service needs may result in this requirement being exempt on some end instruments.

   b. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI, LS]** The product shall not allow the user to access a resource unless that user's user ID has an appropriate privilege to access that resource.

      NOTE: ROUTINE and above VVoIP sessions may be authorized for all users of the system and this feature may be disabled if the systems are located in secure facilities for precedence sessions.

      (1) **[Required: LSC, MFSS, SS]** The product shall only forward a signaling message when the forwarding destination is authorized.

         NOTE: This is to ensure that sessions are not forwarded to an unauthorized destination. This includes on-net and off-net destinations.

   c. **[Required: R, LS, EBC, RSF]** The product shall be capable of regulating remote access by employing positive technical controls such as proxies and screened subnets.

NOTE: Proxies and screened subnets are provided using border controllers, access control lists, firewalls, and virtual LANs.

d. **[Required: R, LS, EBC, RSF]** The product shall be capable of configuring proxies and screened subnets to limit access to only approved, network service classes and configured traffic levels for the authenticated users and end instruments.

NOTE: Proxies and screened subnets are provided by using border controllers, access control lists, firewalls, and virtual LANs. Network service classes are defined by the QoS WG, and they may consist of voice, video, and data service classes.

(1) **[Required: R, LS, EBC, RSF]** The product shall have the capability of controlling the flow of traffic across an interface to the network based on the source/destination IP address, source/destination port number, DSCP, and protocol identifier ("6 tuple").

(a) **[Required: EBC, RSF]** The product shall have the capability of opening and closing "gates/pinholes" (i.e., packet filtering based on the "6 tuple") based on the information contained within the SDP body of the AS-SIP messages.

i. **[Required: EBC, RSF]** The product shall have the capability to close a "gate/pinhole" based on a configurable media inactivity timer and issue a BYE message to upstream and downstream AS-SIP signaling appliances (lost BYE scenario).

NOTE: The inactivity timer is based on the inactivity of the media stream.

A. **[Required: EBC, RSF]** The default media inactivity value for closing a session and issuing BYE messages shall be 15 minutes.

(b) **[Required: R, EBC, RSF]** The product shall have the capability of permitting the configuration of filters that will permit or deny IP packets on the basis of the values of the packet's source address, destination address, protocol, source port, and destination port in the packets header. These filters shall have the capability of using any one value, all values, or any combination of values. Filters using source ports and destination ports shall have the capability to be configured to use ranges of values defined by the operators (1) equal to, (2) greater

than, (3) less than, (4) greater than or equal to and (5) less than or equal to.

(2) **[Required: R, LS]** The product shall be capable of utilizing VLANs to segregate VVoIP and data traffic. Servers requiring access to multiple VLANs shall be kept in a DMZ connected to the firewall and separating the two VLANs.

NOTE: For the purposes of this UCR 2008, all streams of packets associated with a VTC session are considered video to include voice, video, and data streams. A DMZ, in this context, may exist between two VLANs within the Edge Segment.

(a) **[Required: R, LS]** The product shall be capable of supporting a minimum of five distinct VLANs for VVoIP.

(b) **[Required: LS, R]** The product shall be capable of ensuring that EIs (that do not contain a multi-port switch) and VVoIP appliances are only connected to switch ports with access to the VVoIP VLAN(s).

NOTE: This requirement is not applicable to an EI with an embedded multi-port switch.

(c) **[Conditional: EI ~~and~~, AEI]** If the product supports a data workstation, then the system shall be capable of supporting 802.1Q Trunking to separate VVoIP and data traffic, or it shall have a separate Network Interface Card (NIC) for the data and the VVoIP.

NOTE: The intent of this requirement is to prevent the workstation from accessing or viewing the voice traffic as well as to prevent the workstation from accessing the EI and AEI for configuration purposes.

i. **[Conditional: EI, AEI]** If the product supports a data workstation, then the system shall be capable of using separate 802.1Q VLAN tags for VVoIP and data or shall use separate NICs for the data and VVoIP interfaces.

ii. **[Conditional: EI, AEI]** If the product supports a data workstation, then the system shall be capable of routing the VVoIP and data traffic to the appropriate VLAN.

NOTE: This requirement differs from the previous requirement in

that the previous requirement involves marking the packet and this requirement is focused on what action to take based on the marking or the output NIC.

iii. **[Conditional: EI, AEI]** If the product supports a data workstation, then the system shall be able to disable the switchport that allows access for the data workstation when the data workstation is not connected.

(d) **[Required: R, LS]** The product shall be capable of configuring the maximum number of MAC addresses that can be dynamically configured on a given switch port (e.g., 1-3).

i. **[Required: R, LS] [Alarm]** The product shall be capable of notifying the NMS when the MAC address tables threshold is reached to avoid an overflow.

ii. **[Required: R, LS] [Alarm]** The product shall have the capability to generate an alarm to the NMS when an unauthorized MAC address is detected on switchport or the maximum number of MAC addresses allowed on a switch port is exceeded.

(e) **[Required: R, LS]** The product shall be capable of segregating softphones to a dedicated VLAN.

(f) **[Required: R, LS]** The product shall be capable of segregating signaling appliances to a dedicated VLAN.

(g) **[Required: R, LS]** The product shall be capable of segregating PSTN gateways to a dedicated VLAN.

(h) **[Required: R, LS]** The product shall be capable of segregating NMS appliances on a separate VLAN.

(3) **[Required: R, LS, EBC, RSF]** The product shall have the capability to deploy on a dedicated IP network(s) or subnetwork(s) that utilize separate address blocks from the normal data address blocks thus allowing traffic and access control via firewalls and router ACLs.

(a) **[Required: EBC]** The product shall be capable of using NAT and NAPT on all VVoIP enclave to WAN connections.

i. **[Required: R, EBC, RSF]** The product shall have the capability to deploy using private address space in accordance with RFC 1918.

ii. **[Required: EBC]** The EBC shall be an AS-SIP intermediary in all WAN signaling sessions.

A. **[Required: EBC]** To enable the application of NAT and NAPT, the EBC shall be able to inspect and modify the SDP body (i.e., the SDP "c=" and the "m=" lines) of the corresponding AS-SIP message.

iii. **[Conditional: EBC]** If the system supports H.323 video sessions, the EBC shall be capable of supporting H.323 NAT and NAPT.

(b) **[Required: R, LS]** The product shall have the capability to be configured to ensure that the data network perimeter (i.e., data edge router or data perimeter firewall) blocks all external traffic destined to or sourced from the VVoIP VLANs and/or IP address space.

NOTE: The VVoIP VLANs may include a softphone VLAN, a non-softphone voice VLAN, and a video VLAN.

(c) **[Required: R, LS, EBC, RSF]** The product shall have the capability to limit management appliance access to the IP addresses of appropriate workstations.

(4) **[Conditional: R, LS]** If DHCP is used, the product shall have the capability to deploy different DHCP servers for VVoIP and non-VVoIP components and the DHCP servers shall be located on physically diverse platforms from the routers and LAN switches.

(5) **[Conditional: R, LS]** If DHCP is used, DHCP servers shall reside in their respective VVoIP or non-VVoIP address space and the DHCP servers shall be located on physically diverse platforms from the routers and LAN switches.

(a) **[Conditional: R, LS, EI ~~and~~, AEI]** If DHCP is used, the product shall be capable of using 802.1X in combination with a secure EAP type (EAP-TLS, EAP-TTLS, or PEAP) residing on the authentication server and within the operating system or application software of the EI and AEI in order to authenticate to the LAN.

i. **[Conditional: R, LS]** If 802.1X port authentication is used, the product shall ensure that all access ports start in an unauthorized state. NOTE: The product should set AuthControlledPortControl equal to Auto mode for ports that will support VVoIP.

ii. **[Conditional: R, LS, EI ~~and~~, AEI]** If 802.1X port authentication is used, the product shall ensure that reauthentication occurs every 60 minutes.

(6) **[Required: RSF]** The product shall be capable of being configured to ensure that VVoIP and non-VVoIP traffic between their respective VLANs is filtered and controlled such that traffic is restricted to planned and approved traffic between authorized devices using approved ports, protocols, and services.

(7) **[Required: EBC, RSF]** The product shall have the capability to deploy VVoIP aware firewalls at all VVoIP security boundaries (internal and external).

(a) **[Required: EBC, RSF]** The product firewalls deployed at the boundaries of the VVoIP enclave shall have the capability to employ stateful packet inspection.

(b) **[Required: R]** The product shall be capable of implementing traffic conditioning at all VVoIP enclaves associated with the product.

NOTE: This includes limiting the bandwidth associated with external sessions.

e. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI, LS]** The product documentation shall list all of the IP ports and protocols required by the product and the boundaries they transit as defined in the PPS Assurance Category Assignments List and which is maintained by DISA and is described in DODI 8551.1.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI, LS]** The product shall use IP ports and protocols deemed "green" or "yellow" as defined by the PPS Assurance Category Assignments List, which is maintained by DISA and is described in DODI 8551.1.

f. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** Products that support critical commands, operational commands or critical objects shall be capable of establishing access privileges for these objects and commands. Critical objects include authentication data storage.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The default policy on a product that supports operations-related or critical commands shall be capable of disallowing command issuance unless the issuer has been authenticated and authorized to use that command.

(a) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** Assigning passwords to specific actions (e.g., operations-related commands) shall not be used as a primary access control method (though passwords may be used to augment other access control(s).

NOTE: When passwords are used as the primary access control method, confidentiality is lost because of password sharing among authorized users.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** All ports of the product that accept operations-related or critical command inputs shall be capable of exercising system access control. This includes ports that provide direct access, dial-up access, access via a wireless interface, network access, and access via a Data Communications Channel (DCC) as in the case of an Add Drop Multiplexer (ADM) in a SONET.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** Depending on the application, if the product is to be accessed by administrative users who need to keep this access (including the fact that an access is being made) confidential from other administrative users, such as unauthorized B/P/C/S Director of Information Management (DOIM) employees (i.e., CALEA type requirements), the product shall be capable of providing a separate interface/port for such confidential access. It shall be capable of ensuring that messages (including login requests) at this "special" interface/port are kept confidential from users logged on at other interfaces/ports.

NOTE: It is acceptable to implement the CALEA logging functions in a separate security log on a different appliance than the normal security log.

(b) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of controlling access to resources over a given interface/port on the basis of privileges assigned to that interface/port.

(c) **[Conditional: EBC, RSF]** If the product supports CALEA functions, those functions shall be disabled by default.

g. **[Required: R, LS, EBC, RSF]** The product shall have the capability of monitoring the flow of traffic across an interface to the network.

h. **[Required: MFSS, SS, LSC, MG]** The product shall have the capability to provide a secure method for allowing automatic interconnections.

NOTE: Automatic interconnection is only allowed between an incoming long-distance SBU voice call and the local commercial system (off-netting).

(1) **[Required: MFSS, SS, LSC, MG]** Automatic interconnection between DoD IP VVoIP calls and local commercial systems shall only be permitted with proper authorization.

NOTE: The authorization is granted based on successful authentication in combination with an acceptable profile allowing the interconnection.

(2) **[Required: MFSS, SS, LSC, MG]** The product shall have the capability of identifying all calls made through the automatic interconnection.

(3) **[Required: MFSS, SS, LSC, MG]** The product shall be capable of ensuring that all automatic calls are periodically verified by the user.

i. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The NMS shall possess read-access and limited write/controlled access capabilities unless Service/agency operational command personnel are available to make changes around-the-clock to all DoD IP VVoIP database tables (excluding tables associated with non-DISA controlled devices).

NOTE: The intent of this requirement is to ensure that authenticated and authorized NMS personnel have limited capability to resolve issues in the event that a problem occurs and there are no on-site maintenance personnel available.

~~j. **[Required: MFSS, SS, LSC, MG, EBC, RSF]** The product shall have the capability to provide an identification system that allows the operators to detect and prevent disruptive fraud, abuse, and compromise within 30 minutes. (Definition of disruptive is found in UCR 2008, Appendix A, Definitions, Abbreviations and Acronyms, and References.)~~

~~NOTE: The threats associated with this requirement are summarized earlier in this UCR 2008.~~

~~(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF]** The product shall have an identification system that allows operators to detect a disruptive fraud, abuse, or compromise within 5 minutes.~~

~~NOTE: The threats associated with this requirement are summarized earlier in this UCR 2008 section.~~

k. **[Required: MFSS, SS, LSC, EBC, RSF]** The product shall have the capability to deny system access to all session requests (i.e., disable the points of ingress) in response to appropriate messages received from the NMS.

NOTE: Sessions in this context are associated with NMS sessions, such as a SSH session.

l. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** If the product provides an emergency entry port (Emergency Action Interface) with system access control, the product shall have the capability to meet the following requirements (note that an emergency port is defined to be a port that is infrequently used and therefore it is not utilized for the purposes of regular maintenance):

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of minimally using ~~strong authentication~~a username with a strong password which meets the complexity and character diversity requirements specified in this UCR.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall log all access attempts in an audit log.

(3) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of ensuring at least one, and not more than two, system security administrator accounts cannot be locked out due to login failures.

m. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** If the product provides an emergency entry port without system access control then the following requirements shall be met.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product emergency entry port shall recognize only those commands that perform

system restoration (for example, from a disk) and no other operations commands.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS] [Alarm]** The product shall generate a real time alarm/alert when this port is used to gain access to the system and transmit that alarm to the appropriate NOC.

n. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall have the capability to deny the establishment of any session via a port that is not designed to accept operations-related command inputs. For example, if the output port receives a login request, the system shall not respond.

o. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN]** The product shall be capable of providing a time-out feature for users of the product. This implies that, if during a session, there has not been any exchange of messages for a specified period or some other away-from-console event occurs, the product shall lock out that session for subsequent inputs (or reauthenticate user before accepting subsequent inputs).

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The default for session inactivity is 15 minutes and shall be configurable.

(2) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF]** If the product uses a keyboard, the product shall be capable of providing a mechanism for user-initiated keyboard locking. When a keyboard is locked, the session time-out feature shall be suspended. The unlocking of a locked keyboard shall require authentication (e.g., entering the password). When the keyboard is unlocked, the session time-out feature shall be resumed.

(3) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF]** If the ~~v~~product does not use a keyboard (i.e., SSH or other type of remote NMS session), the product shall terminate the session and automatically log the user out after the session inactivity timer has expired.

p. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of providing a mechanism to end a user session through a secure log off procedure. This implies that when a user terminates a session by logging off, the product shall be capable of ensuring that the port drops immediately and the processes running at the time of logoff are terminated. When a subsequent user attempts to log on to that port, the user shall be required to go through the entire login procedure including identification and authentication, and shall not be granted automatic access (i.e., bypassing the login procedure) to any process invoked by the previous user.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The system shall invalidate session identifiers upon user logout or other session termination.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** For graphical interfaces (e.g. non command line based, such as a web page), the system shall provide a logout capability that is readily observable to the user.

q. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of dropping a port if a session is interrupted due to reasons such as time-out, power failure, link disconnection, etc., and the same login procedure as described ~~above~~in the previous requirement shall be required of a subsequent session request.

NOTE: Serial ports must drop the session immediately. A delay in dropping the session may occur with Ethernet connections due to the nature of the TCP keep alive capabilities that may appear to keep the session alive. When the disconnected Ethernet connection is attempted to be used to pass data, the connection should drop. If the session drop is not induced by the application, the session should eventually drop on its own once the keep alive fails.

r. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** Depending on the application, if the product employs external modems to perform dial/dial-back, the corresponding modems shall be capable of having the following characteristics:

(1) The modem, after receiving a call from a session requester, shall disconnect the line before dialing the authorized number to reestablish the contact.

(2) The dial-back shall be performed over a line different from the line over which the session request arrived at the modem.

(3) A loss of power to the modem shall not cause the modem to fall back to a default password.

(4) The password file in the modem shall not be readable by a user.

(5) The modem shall prevent any modification of its stored configuration unless the user attempting this modification is properly authenticated and found to be authorized for this action.

s. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of limiting the access to newly created resources in conformance with the privilege of the creator of the resource. This should be the default configuration.

t. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** If the application requires the product to provide different interfaces/ports for different functions, access to product resources over a given interface/port shall be controlled on the basis of privileges assigned to that interface/port.

u. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of providing a level of granularity such that, for any specified resource controlled by the system (to include precedence calls), it shall be possible to do the following:

(1) Grant access rights to a specified user/customer or group of users/customers.

(2) Deny access rights to a specified user/customer or a group of users/customers.

(3) Grant access rights to a specified interface/port or a group of interfaces/port.

(4) Deny access rights to a specified interface/port or a group of interfaces/ports.

(5) Deny a user access to potentially damaging processes and transactions that the user does not have to access to be functional.

(6) Deny an interface/port access to potentially damaging processes and transactions that the interface/port does not have to access to be functional.

(7) Deny a user (as well as an interface/port) access to data files and/or tables unless the user (as well as the interface/port) is authorized for it.

(8) **[Conditional]** If the system has its operations database structured based on commands, views, records, and fields, the system shall restrict, based on user ID as well as interface/port, the execution of any specifiable command on any specifiable view, record, or field.

v. **[Required: FW, IPS, VPN]** The security device shall only allow authorized security personnel to configure alert mechanisms.

w. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** Systems that generate and assign session identifiers for each new session shall generate unique session identifiers using a randomizer conforming to NIST requirements.

NOTE: The intent is to ensure that it is extremely difficult for an adversary to guess a valid session identifier.

5.4.6.2.2 Integrity

1. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI, LS]** The product shall be capable of providing data and system integrity.

   a. **[Required: MFSS, SS, LSC, MG, EBC, RSF, AEI, EI]** The product shall be capable of ensuring the integrity of signaling messages.

      (1) **[Required: MFSS, SS, LSC, EBC, RSF, AEI – Conditional: EI]** The product shall be capable of using TLS for providing integrity of AS-SIP messages.

      NOTE: The condition for the EI is the support of AS-SIP.

         (a) **[Required: MFSS, SS, LSC, EBC, RSF, AEI – Conditional: EI]** The product shall be capable of using HMAC-SHA1-160 with 160 bit keys.

      (2) **[Conditional: MFSS, SS, LSC, EI ~~and~~, AEI]** If the product uses H.323, the product shall be capable of using H.235.1 Baseline Security Profile guidance for mutually authenticated shared keys and HMAC-SHA1-96 with 160 bit keys.

   b. **[Required: MFSS, SS, LSC, MG, EBC, RSF]** The products shall be capable of protecting data integrity by performing integrity checks and/or data updates. Examples include:

      (1) Proper rule checking on data update

      (2) Adequate alert messages (e.g., “Do you really mean it?”) in response to potentially damaging commands before executing them, so that involuntary human errors may be reduced.

      (3) Proper handling of duplicate/multiple inputs

      (4) Checking return status

      (5) Checking intermediate results

      (6) Checking inputs for reasonable values

      (7) Proper serialization of update transactions.

c. **[Required: MFSS, SS, LSC, MG, EBC, RSF] [Alarm]** The product shall be capable of providing mechanisms or procedures that can be used to periodically validate its correct operation (such as proper functioning of the security log, proper functioning of various trigger mechanisms, etc.) and the product shall alert the NMS when anomalous operation is detected.

d. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of providing mechanisms to monitor system resources and their availabilities (e.g., overflow indication, lost messages, and buffer queues).

e~~.~~. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS] [Alarm]** The product shall be capable of providing mechanisms to detect communication errors (relevant to the system) above a specifiable threshold. The product shall be capable of providing a configurable capability to alarm when critical errors (relevant to the system) are detected.

NOTE: The types of communications errors that must be detected include abnormally large numbers of received packets that fail decryption and/or fail to pass integrity checks (e.g. failed CRC or hash function computations).

f. **[Required: MFSS, SS, LSC, EBC, RSF]** The product shall be capable of providing a mechanism to monitor the integrity of the system and generate a status report detailing the values of all parameters and flags that affect the secure operation of the system.

NOTE: The vendor shall document parameters and flags that affect the secure operation of the product and the Information Assurance test team will provide technical advisement to the DSAWG regarding their adequacy.

(1) **[Required: MFSS, SS, LSC, EBC, RSF] [Alarm]** The system shall support the capability to generate an alarm to the NMS when it detects that the integrity of the system is such that it is no longer operating in an approved or secure state. (Example: A failed signature check on the currently loaded software would cause this type of alarm)

g. **[Required: MFSS, SS, LSC, MG, EBC, RSF]** The product shall be capable of automatically running file or disk integrity checking utilities by vendor-supplied software.

h. **[Required: EI, AEI, MG, MFSS]** The product shall be capable of providing data integrity of the bearer (Transport) packets.

(1) **[Required: EI, AEI, MG, MFSS]** The product shall be capable of using HMAC-SHA1-32 for the authentication tag with 160 bit key length as the default integrity mechanism for SRTP packets.

(2) **[Required: EI, AEI, MG, MFSS]** The product shall be capable of using HMAC-SHA1-80 for the authentication tag with 160 bit key length as the default integrity mechanism for SRTCP.

NOTE: The ~~use of this protocol~~ability to process received SRTCP messages is optional, but the capability to transmit SRTCP messages is required.

i. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** Products that support remote network management functions and/or critical network resources and services shall be capable of providing appropriate standard (FIPS 140-2) cryptography based data integrity services to protect and detect against unauthorized modification of messages.

j. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** An appliance and its applications shall be capable of ensuring that it cannot be made to enter an insecure state as a result of the operation of non-privileged code.

NOTE: It is understood that systems shall satisfy this requirement using industry best practices and will mitigate any findings associated with this requirement discovered during Information Assurance testing.

k. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall be capable of ensuring that default user IDs and passwords, previously modified by the administrator, do not revert to the vendor delivered default user IDs and passwords when the system is restarted unless configured to do so by an appropriate administrator.

l. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS]** The product shall be capable of providing mechanisms to ensure the integrity of the data that is stored on the appliance and is used to support authentication processes. This includes protecting the information from malicious deletion, modification, or insertion. NOTE: Examples of the data stored would be private keys or certificates.

m. **[Conditional: MFSS, SS, LSC, MG]** If the product uses IPSec, the product shall be capable of using HMAC-SHA (class value 2) as the default IKE integrity mechanism as defined in RFC 2409.

n. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The entire SNMPv3 message shall be checked for integrity and shall use the HMAC-SHA1-96 with 160 bit key length.

o. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** If the product uses SSHv2, the product shall use HMAC-SHA1-96 with 160 bit key length for data integrity.

p. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI]** If the product uses TLS, the product shall be capable of using TLS (SSLv3.1 or higher) in combination with HMAC-SHA1-160 with 160 bit keys to provide integrity for the session packets.

2. **[Required: FW, IPS, VPN]** The security device shall be capable of providing data and system integrity.

a. **[Required: FW]** The security device, when acting as an IPSec Gateway, will perform Authentication Header key checks.

b. **[Required: FW, IPS, VPN]** The security device shall use industry-accepted integrity mechanisms such as parity checks and cyclic redundancy checks (CRCs).

c. **[Required: FW, IPS, VPN]** The security device system assurance shall include features and procedures to validate the integrity and the expected operation of the security relevant software, hardware, and firmware.

d. **[Required: FW, IPS, VPN]** System initialization, shutdown, and aborts shall be configured to ensure that the system remains in a secure state.

e. **[Required: FW, IPS, VPN]** The security device system assurance shall include control of access to the security support structure (i.e., the hardware, software, and firmware that perform operating system or security functions).

f. **[Required: IPS, VPN]** Data and software storage integrity protection, including the use of strong storage integrity mechanisms (e.g., integrity locks, encryption) shall be employed.

g. **[Required: IPS, VPN]** Procedures to prevent the introduction of malicious code into the system, including the timely updating of those mechanisms intended to prevent the introduction of malicious code (e.g., updating anti-viral software) shall be employed.

h. **[Required: FW, IPS, VPN]** Security devices shall at a minimum use HMAC-SHA1 for hashing operations.

5.4.6.2.3 Confidentiality

1. **[Required: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS]** ~~The product~~Products providing encryption services shall be capable of providing data and signaling confidentiality. (This includes protection for all VVoIP signaling and media traffic~~.~~.)

   a. **[Required: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS, FW, IPS, VPN]** The product shall at a minimum implement FIPS 140-2 Level 1 validated cryptographic hardware modules or software toolkits ~~operated~~and operate this module in a FIPS ~~Mode~~140-2 approved mode for all encryption mechanisms.

      NOTE: FIPS 140-2 addresses many aspects of the cryptographic module to include the encryptor and the random number generator. The application does not have to be FIPS 140-2 compliant, but the cryptographic module within the application must be compliant. It is expected that a vendor either will purchase an approved FIPS 140-2 cryptographic module for their application or will submit their developed cryptographic module to an approved FIPS 140-2 certification laboratory before submitting their solution to the Government for testing. It is anticipated that the Government will accept a LOC from a vendor as a means of satisfying this requirement.

      (1) **[Optional: FW, IPS, VPN]** Security devices that provide encryption services shall be FIPS 140-2, Level 2 compliant.

      (2) **[Optional: FW, IPS, VPN]** Where encryption is employed, the security device shall provide the capability to implement an internal cryptographic function to verify the integrity of all security function executable code and data except the following: audit data, or other dynamic security function data for which no integrity validation is justified.

   b. **[Required: EI, AEI, MG]** The product shall be capable of providing confidentiality for media streams using SRTP with either the AES_CM_128 encryption algorithm as the default or **[Required UCR ~~2010~~2012]** AES 256-bit algorithm.

      (1) **[Required: EI, AEI]** ~~The~~To support SRTP, the product shall be capable of generating keys using a random source algorithm that meets the requirements of ~~FIP 186 to support SRTP.~~:

         a. FIPS 186 if the product's randomizer is approved by NIST before and including 2010

b. NIST SP 800-90 if the product's randomizer is approved by NIST after 2010

NOTE: At the time of this document's writing, draft NIST SP 800-131 fully deprecates FIPS 186 randomizers after the year 2015.

(2) **[Required: MFSS, SS, LSC, MG, EI, AEI]** The product shall be capable of distributing the Master Key and the Salt Key in the VVoIP signaling messages in accordance with RFC 4568.

(3) **[Required: MFSS, SS, LSC, MG, EI, AEI]** The product shall be capable of distributing the Master Key and the Salt Key in concatenated form.

(4) **[Required: EI, AEI, MG]** The product shall use a Master Key of 128 bits in order to support 128-bit AES encryption.

NOTE: This implies that the Master Salt Key may be null.

(5) **[Required ~~UCR 2010:~~ : EI, AEI, MG]** The Master Key and a random Master Salt Key shall be supported for SRTP sessions.

~~NOTE: This is in addition to the 256-bit requirement.~~

c. **[Required: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI]** The product shall be capable of providing confidentiality for signaling messages using TLS or IPSec (or its equivalent) using either:

AES 128-bit algorithm or **[Required UCR 2012]** AES 256-bit algorithm.

(1) **[Conditional: MFSS, SS, LSC, MG, EI ~~and~~, AEI]** If H.323, MGCP, or H.248 (MEGACO) is used, the product shall be capable of using IPSec to provide confidentiality.

(a) **[Conditional: MFSS, SS, LSC, MG]** If the product uses H.248 (MEGACO), the product shall be capable of distributing the SRTP Master Key and Salt Key in the SDP "k =" crypto field when using H.248.15.

(b) **[Conditional: MFSS, SS, LSC, MG, EI ~~and~~, AEI]** If H.323 is used, the product shall be capable of distributing the SRTP Master Key and

Salt Key in H.235 using the H235Key as described in H.235.0 and H.235.8.

(c) **[Conditional: MFSS, SS, LSC, MG, EI, AEI]** If IPSec is used, the product shall be capable of using IKE for IPSec key distribution:

i. **[Required: MFSS, SS, LSC, MG, EI, AEI]** IKE version 1

ii. **[Required: MFSS, SS, LSC, MG, EI, AEI]** IKE version 2 (IKEv2)

NOTE: IKEv2 requirements are found in UCR 2008, Section 5.3.5, IPv6 Requirements. Section 5.3.5 also contains the timeframe for when IKEv2 is required (whether in this UCR or in future UCR revisions).

iii. **[Conditional: MFSS, SS, LSC, MG, EI, AEI]** If IPSec is used, the product shall be capable of using the Revised Mode of public key encryption during Phase I of the ISAKMP negotiation for authentication.

iv. **[Conditional: MFSS, SS, LSC, MG, EI, AEI]** If IPSec is used, the product shall be capable of using the Quick Mode as the default Phase II authentication mechanism.

v. **[Conditional: MFSS, SS, LSC, MG, EI, AEI]** If IPSec is used, the product shall be capable of using and interpreting certificate requests for PKCS#7 wrapped certificates as a request for the whole path of certificates.

vi. **[Conditional: MFSS, SS, LSC, MG, EI, AEI]** If IPSec is used, the product shall be capable of using Main Mode associated with the Diffie-Hellman approach for key generation for the security association negotiation.

A. **[Conditional: MFSS, SS, LSC, MG, EI, AEI]** If IPSec is used, the product shall only support the following erroneous messages associated with a certificate request:

1. Invalid Key

2. Invalid ID
3. Invalid certificate encoding
4. Invalid certificate
5. Certificate type unsupported
6. Invalid CA
7. Invalid hash
8. Authentication failed
9. Invalid signature
10. Certificate unavailable

vii. **[Conditional: MFSS, SS, LSC, MG, EI, AEI]** If IPSec is used, the product shall be capable of using Oakley Groups 1, 2, and ~~2~~2048 as a minimum.

(d) **[Conditional: MFSS, SS, LSC, MG, EI, AEI]** If IPSec is used, the product shall be capable of using AES_128_CBC as the default encryption algorithm.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, AEI – Conditional: ~~-~~ EI]** The product shall be capable of using TLS (dual path method) to provide confidentiality for the AS-SIP.

NOTE: Upon receipt of an INVITE over a TLS-established session, an LSC shall respond to the INVITE (and any subsequent requests received over that TLS path) using this TLS session. If the LSC originates an INVITE or request, then it shall establish a separate and unique TLS session, and the LSC shall expect to receive a response to its request over this new TLS session. Two TLS sessions are established for communications between the LSC and the EBC, MFSS and EBC, LSC and LSC, LSC to AEI via RSF, or EBC and EBC. Since the AEI is required to support the dual path method it has to act as both a SIP client and server. Due to the proprietary nature of line-side IP solutions, vendors may support TLS reuse or the dual path method described above for line side implementations. The details associated with the dual path method are described in http://tools.ietf.org/html/rfc5923~~http://tools.ietf.org/html/draft-ietf-sip-connect-reuse-14~~.

NOTE: The condition for the EI is the support of AS-SIP.

(a) **[Required: MFSS, SS, LSC, MG, EBC, RSF, AEI – Conditional: EI]** The underlying protocol for AS-SIP shall be the TCP.

(b) **[Required: MFSS, SS, LSC, MG, EBC, RSF, AEI – Conditional: EI]** The product shall be capable of using as its default cipher either:

[Conditional] TLS_RSA_WITH_AES_128_CBC_SHA or

[Required UCR ~~2010~~2012]
TLS_RSA_WITH_AES_256_CBC_SHA

(c) **[Required: MFSS, SS, LSC, MG, EBC, RSF, AEI – Conditional: EI]** The product shall be capable of using a default of no compression for AS-SIP messages.

(d) **[Required: MFSS, SS, LSC, MG, EBC, RSF, AEI – Conditional: EI]** The product shall be capable of exchanging AS-SIP TLS messages in a single exchange or multiple exchanges.

(e) **[Required: MFSS, SS, LSC, MG, EBC, RSF, AEI – Conditional: EI]** The product shall be capable of distributing the SRTP Master Key and Salt Key in the AS-SIP message using the SDP crypto= field. NOTE: EI condition is whether it supports AS-SIP.

(f) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, AEI, EI]** If TLS session resumption is used, a timer associated with TLS session resumption shall be configurable and the default shall be 1 hour.

NOTE: This requirement is not associated with Network Management related sessions.

i. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, AEI, EI]** If TLS session resumption is used, the maximum time allowed for a TLS session to resume (session resumption) without repeating the TLS authentication/confidentiality/authorization process (e.g. a full handshake) is 1 hour.

(g) **[Conditional: MFSS, SS, LSC, EI, EBC, RSF, AEI]** If AS-SIP is used, the product shall only transmit packets that are secured with TLS and use port 5061.

NOTE: The products may use other signaling protocols for interfacing to MGs, EIs, etc.

(h) **[Required: MFSS, SS, LSC, EI, EBC, RSF, AEI]** The product shall reject all received AS-SIP packets associated with port 5061 that are not secured with TLS.

NOTE: This ensures that the product does not process UDP, SCTP, and TCP SIP packets that are not secured using a combination of TLS and TCP.

(i) **[Required: MFSS, SS, LSC, EI, EBC, RSF, AEI]** The product shall only accept and process AS-SIP packets that arrive on port 5061.

NOTE: The product should discard AS-SIP packets that arrive on a different port.

(j) **[Required: RSF]** The product shall support both the reuse and dual path TLS methods.

NOTE: This is required of a RSF since it has to support TLS sessions between the LSC and AEI and proprietary EIs. The AEI uses the dual path method and proprietary EIs have the option of using the reuse method.

(k) **[Conditional: MFSS, SS, LSC, MG, EBC, AEI]** If the system utilizes TLS to transport AS-SIP messages, the system shall support the use of the keep alive mechanism described in RFC 5626 in order to avoid closure of the TLS given session due to inactivity.

i. **[Conditional: MFSS, SS, LSC, MG, EBC, AEI]** If the system utilizes TLS to transport AS-SIP messages, the system shall support the transmission of the four character "carriage return-line feed-carriage return-line feed" sequence, described in Section 4.4.1 of RFC 5626, based on a configurable inactivity timer.

NOTE: This inactivity timer would reset every time a new AS-SIP message is transmitted. The maximum value of this timer would be pre-configured or optionally determined from a received RFC 5626 "Flow-Timer" header in a REGISTER messsage (in the case of an AEI or EI).

ii. **[Conditional: MFSS, SS, LSC, EBC]** If the system utilizes TLS to transport AS-SIP messages, the system shall support the capability to respond to a received "carriage return-line feed-

carraige return-line feed" sequence by sending the two character "carriage return-line feed" sequence, in accordance with RFC 5626 Section 4.4.1.

d. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, AEI, EI, ~~AEI~~FW, IPS, VPN]** If the product uses web browsers or web servers, the product web browsers and web servers shall be capable of supporting TLS (SSLv3.1) or higher for confidentiality.

e. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of using SSHv2 or TLS (SSLv3.1) or higher for remote configuration of appliances.

NOTE: EIs and AEIs remote manual configurations shall not be enabled and all non-automatic processes shall be performed locally.

f. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, ~~EI~~R, LS, AEI, EI]** If the product uses TLS, the product shall do so in a secure manner as defined by the following subtended requirements.

(1) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI]** If the product uses TLS, the system shall be capable of using TLS_RSA_WITH_AES_128_CBC_SHA or TLS_RSA_WITH_AES_256_CBC_SHA **[REQUIRED UCR ~~2010~~2012]** as its default cipher.

(2) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, ~~EI~~R, LS, AEI, EI]** If the product uses TLS, the system shall be capable of using a default of no compression.

(3) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, ~~EI~~R, LS, AEI, EI]** If the product uses TLS, the system shall be capable of exchanging TLS messages in a single exchange or multiple exchanges.

(4) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, ~~EI~~R, LS, AEI, EI]** If TLS session resumption is used, a timer associated with TLS session resumption shall be configurable and the default shall be 1 hour.

NOTE: This requirement is not associated with NM-related sessions.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, ~~EI~~R, LS, AEI, EI]** If TLS session resumption is used, the maximum time allowed for a

TLS session to resume (session resumption) without repeating the TLS authentication/confidentiality/authorization process is 1 hour.

(5) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, AEI, EI]** If the product supports SSL/TLS renegotiation, the product shall support the capability to disable this feature or the product shall support RFC5746.

NOTE: Supporting RFC 5746 includes providing a configurable option to terminate a TLS session if the peer does not support the 'renegotiation_info' extension.

g. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS]** If the product uses SSH, the system shall do so in a secure manner as defined by the following subtended requirements.

NOTE: EIs remote manual configurations shall not be enabled and all non-automatic processes shall be performed locally.

(1) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS]** If the product uses SSH, the system shall be capable of supporting the RSA 2,048-bit key algorithm~~.~~ and the Diffie-Hellman 2,048 bit key algorithm.

(2) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS]** If the product uses SSH, the system shall use SSH in a secure manner.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS]** If the product uses SSH, a client shall close the session if it receives a request to initiate a SSH session whose version is less than 2.0.

NOTE: Closing the session may be either a default behavior or a configurable option. If this is a configurable option, the conditions of fielding should clearly specify that this option must be configured.

(b) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS]** If the product uses SSH, SSH sessions shall rekey at a minimum every gigabyte of data received or every 60 minutes, whichever comes sooner. ~~If the product uses SSH, SSH sessions shall rekey at a minimum every 2^{31} of transmitted data or every gigabyte of data, or every 60 minutes.~~

(c) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS]** If the product uses SSH, SSH sessions shall rekey at a minimum every

gigabyte of data transmitted or every 60 minutes, whichever comes sooner.~~If the product uses SSH, SSH sessions shall transmit less than 2^{32} packets or no more than a gigabyte of data after a key exchange has occurred.~~

(d) **[Reserved]**

~~(d) [Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS] If the product uses SSH, SSH sessions shall rekey at a minimum after receiving 2^31 packets, or every gigabyte of data, or every 60 minutes.~~

(e) **[Reserved]**

~~(e) [Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS] If the product uses SSH, SSH sessions shall accept less than 2^32 packets or no more than a gigabyte of data after a key exchange has occurred.~~

~~NOTE: These requirements are consistent with the SSHv2 recommendation formula for the number of packets to accept (2(L/4) where L is the key length – 128 bits).~~

(f) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS]** If the product uses SSH, the SSH sessions shall minimally support the following encryption algorithms defined in RFC 4253 and RFC 4344:~~If the product uses SSH, SSH sessions shall use as the default encryption algorithm either:~~

- AES128-CTR,
- AES128-CBC (for backwards compatibility with older UCR versions),
- and **[Required UCR 2012]** AES256-CTR.

i. **[Conditional: MFSS, SS, LSC, MG, EBC, EI, AEI, R, LS]** If the product uses SSH, SSH sessions shall use as the default (most preferred) encryption algorithm either:

AES128-CTR or **[Required UCR 2012]** AES256-CTR

~~AES128-CBC or **[UCR 2010]** AES256-CBC .~~

(g) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS]** If the product uses SSH, SSH sessions shall use TCP as the underlying protocol.

(h) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS]** If the product uses SSH, it shall be capable of processing packets with uncompressed payload lengths up to 32,768 bytes or shall be configurable to specific that value; this length shall also be the default value ~~for uncompressed SSH packet payloads. .~~ This does not preclude the system from automatically sizing the MTU if it is less than 32,768.

i. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS]** If the product uses SSH, SSH packets shall have a maximum packet size of 35,000 bytes or shall be configurable to that value; this length shall also be the default value.

NOTE: the 35,000 bytes includes the packet_length, padding_length, payload, random padding, and MAC.

ii. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS]** If the product uses SSH, the product shall discard SSH packets that exceed the maximum packet size to avoid denial of service attacks or buffer overflow attacks.

iii. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS]** If the product uses SSH, SSH packets shall use random bytes if packet padding is required.

(i) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS]** If the product uses SSH, the system shall treat all SSH encrypted packets sent in one direction as a single data stream. For example, the initialization vectors shall be passed from the end of one packet to the beginning of the next packet.

(j) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS]** If the product uses SSH, the system shall ~~use~~be capable of setting Diffie-Hellman-~~Group1~~Group14-SHA1 as the ~~default~~preferred key exchange mechanism for SSH.

(3) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The use of SSH is conditional, however, if the product uses SSH, ~~beginning in UCR2010,~~ the product using SSH shall be DoD PKE~~.~~ (Public-Key Enabled).

NOTE: EIs and AEIs are excluded from this requirement since remote management of the system is disabled after initial installation.

(a) **[~~Required UCR2010:~~ Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** If the product uses SSH, the system ~~using SSH~~ shall support the capability to use ~~DoD PKI~~ X.509v3 certificates issued by a DoD approved PKI to establish the encrypted sessions.

~~NOTE: X.509v3 is being defined as an additional SSH key type as provided for in RFC 4251 [SSH-ARCH] and discussed in Section 6.6 of RFC-4253 [SSH-TRANS]. X.509v3 Certificates are defined in RFCs 3647 and 5280.~~

(b) **[~~Required UCR 2010:~~ Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** If the product uses SSH and provides an SSH Server function, the SSH server shall support the capability to utilize an X.509v3 certificate provided by a DoD approved PKI.~~If the product uses SSH, the SSH server shall have its own DoD PKI X.509v3 certificate.~~

i. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The SSH Server function shall at a minimum support the "x509v3-sign-rsa" key type as defined in draft-saarenmaa-ssh-x509-00.

NOTE: At the time of this document's writing, this specification can be found at the following URL: http://tools.ietf.org/html/draft-saarenmaa-ssh-x509-00.

NOTE: At this time there is an active draft IETF specification 'draft-igoe-secsh-x509v3' that will address use of SSH with X.509v3 certificates along with SHA-256 to sign data exchanged during SSH session establishment. This may be mandated in a future UCR revision once this RFC is approved.

ii. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The SSH Server function shall support the capability to specify "x509v3-sign-rsa" as the most preferred key type advertised during the SSH_MSG_KEXINIT message exchange.

iii. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The SSH server function shall support the capability to deny SSH

sessions when the client does not support authentication using the "x509v3-sign-rsa" key type or the session fails to negotiate the "x509v3-sign-rsa" key type.

(c) **[~~Required UCR2010:~~ Conditional: MFSS, SS, LSC, MG, EBC, RSF, ~~,~~ R, LS]** If the product uses SSH, the SSH client shall ~~use a DoD PKI~~support the capability to utilize an X.509v3 certificate provided by a DoD approved PKI.

~~(~~i~~)~~ **~~[Required UCR 2010:~~** . **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, ~~,~~ R, LS]** If the product uses SSH and if the SSH client has a CAC (or equivalent) reader, the SSH client may use the ~~DoD PKI~~X.509v3 certificate on the ~~user's~~user's CAC to establish the encrypted session.

~~(~~ii~~)~~ **~~[Required UCR 2010:~~** . **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, ~~,~~ R, LS]** If the product uses SSH and if the client has a CAC reader and also has its own ~~DoD~~PKI certificate from a DoD approved PKI ~~certificate~~, the client may use either its certificate or the certificate on the ~~user's~~user's CAC to establish the encrypted sessions.

(d) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]**~~[Required UCR 2010: MFS S, SS, LSC, MG, EBC, RSF, , R, LS]~~ If the product uses SSH, the SSH server shall validate the DoD approved PKI certificate supplied by the SSH client in accordance with the specifications in PKI Section 5.4.6.2.1.6 of this document.

(e) **[~~Required UCR 2010:~~ Conditional: MFSS, SS, LSC, MG, EBC, RSF, ~~,~~ R, LS]** If the product uses SSH, the SSH client shall validate the SSH server's DoD PKI certificate in accordance with the specifications in PKI Section 5.4.6.2.1.6 of this document.

(f) **[~~Required UCR 2010:~~ Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** If the product uses SSH, the SSH server shall certify and validate the SSH client's DoD approved PKI certificate before establishing an encrypted session.

NOTE: The certification and validation consists of determining that the client's certificate has not expired and has not been revoked. The server shall not establish an encrypted session with a client whose certificate has expired or been revoked.

(g) **[~~Required UCR 2010~~Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** If the product uses SSH, the SSH client shall certify and validate the SSH server's DoD approved PKI certificate before establishing an encrypted session.

(h) **[~~Required UCR 2010~~Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** If the product uses SSH, the system shall disconnect a session if the PKI certificate validation has not been completed within a configurable time period. The default shall be 10 minutes.

(i) **[~~Required UCR 2010: ~~Conditional: MFSS, SS, LSC, MG, EBC, RSF, ~~,~~ R, LS]** If the product uses SSH, the ~~system~~SSH server shall disconnect if the number of failed ~~PKI certificate~~ validation attempts for a single session exceeds a configurable parameter and the default shall be three attempts.

~~NOTE: When the DoD PKI certificates have been validated, the SSH authentication process has been completed. This SSH authentication method is described in Section 7 (Public Key Authentication Method) of RFC 4252 [SSH-AUTH]. As noted in Section 7, the SSH server may require additional authentication after the SSH authentication has been successfully completed. All UCR SSH servers require additional authentication.~~

NOTE: All users must be authenticated in accordance with the specifications presented in the Authentication Practices Section (5.4.6.2.1.5) of this document

h. **[Required: MFSS, SS, LSC, MG, EBC, RSF, ~~,~~ R, LS]** The product shall be capable of using SNMPv3 for all SNMP sessions.

NOTE: If the product is using Version 1 or Version 2 (instead of SNMPv3) with all of the appropriate patches to mitigate the known security vulnerabilities, any findings associated with this requirement may be downgraded. In addition, if the product has also developed a migration plan to implement Version 3, any findings associated with this requirement may be further downgraded.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The security level for SNMPv3 in the DoD VVoIP environment shall be authentication with privacy – snmpSecurityLevel=authPriv. The product shall set

snmpSecurityLevel=authPriv as the default security level used during initial configuration.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The SNMPv3 architecture shall be capable of allowing an appropriate administrator to manually configure the snmpEngineID from the operator console. A default unique snmpEngineID may be assigned to avoid unnecessary administrative overhead, but this must be changeable.

(3) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The security model for SNMPv3 shall be User-Based Security Model – snmpSecurityModel =3.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** If the product receives response messages, the product shall conduct a timeliness check on the SNMPv3 message.

(b) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** An SNMPv3 engine shall perform time synchronization using authenticated messages.

(4) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The message processing model shall be SNMPv3 – snmpMessageProcessingModel=3.

(5) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The default encryption cipher for SNMPv3 shall be CBC-DES-128 – usmDESPrivProtocol – CBC-DES_128.

(a) **[Required UCR 2012: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall support the capability to negotiate the CFB-AES-128 encryption cipher usmAesCfb128PrivProtocol as defined in RFC 3826.

(6) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** If the product receives SNMPv3 response messages, then the SNMPv3 engine shall discard SNMP response messages that do not correspond to any current outstanding Request messages.

(7) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** If the product receives SNMPv3 responses, then the SNMPv3 Command Generator Application shall discard any Response Class PDU for which there is no outstanding Confirmed Class PDU.

(8) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** When using msgID for correlating Response messages to outstanding Request messages, the SNMPv3 engine shall use different msgIDs in all such Request messages that it sends out during a 150 second Time Window.

(9) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** An SNMPv3 command Generator or Notification Originator Application shall use different request-ids in all Request PDUs that it sends out during a Time Window.

(10) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** When sending state altering messages to a managed authoritative SNMPv3 engine, a Command Generator Application should delay sending successive messages to that managed SNMPv3 engine until a positive acknowledgement is received from the previous message or until the message expires.

(11) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product using SNMPv3 shall implement the key-localization mechanism.

i. **[Required: MFSS, SS, LSC, MG, EBC, RSF]** The product shall be capable of ensuring confidentiality by protecting one user's resource from being accessed by others who do not have such authorization.

NOTE: An instance of this is if the system is accessed by users (including third party service providers) who need confidentiality of their respective resources (which may contain proprietary, confidential, or sensitive information) from one another or from unauthorized personnel.

NOTE: If resource control mechanisms such as command control, object control, record control, and field control fail to provide the required confidentiality, it may be necessary to partition the system database to protect one user's data from being accessed by another user.

j. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of using a separate interface for management traffic.

NOTE: The separate interface may be a logically or physically separate interface.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of protecting the management interface using filters.

NOTE: Within a router, the filters may be achieved using ACLs. Within an

appliance, the filters may include internal routing procedures to the different physical interfaces or VLAN tagging.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of using VLANs to segregate management traffic from other types of traffic where feasible. NOTE: The R and LS will implement the VLAN, but the other appliances will have to tag the packets appropriately with the correct VLAN tag.

k. **[Conditional: MFSS, SS, LSC, MG]** If the product uses IPSec, the system shall be capable of using ~~3DES~~AES-CBC ~~(class value 5)~~ as the default IKE encryption algorithm. The system ~~**[Threshold]** AES-CBC **[**~~shall be capable of supporting 3DES-CBC (class value 5) for backwards compatibility with previous UCR ~~**2010]**.~~revisions.

l. **[Conditional: MFSS, SS, LSC, MG]** If the product uses different signaling protocols (i.e., H.323 and AS-SIP), the system shall be capable of translating/ transferring the bearer keys between different signaling protocols.

m. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall rekey each encrypted session once the session has transmitted a maximum of 2^(L/4) blocks of data. L is the block length in bits (e.g., 128 for AES_128) and shall be configurable.

NOTE: This is to prevent birthday property and other modes of attack.

n. **[Conditional: MFSS, SS, LSC, MG, EI, AEI]** If the product is the originating party and receives a 181 message indicating that the call is being forwarded, then upon completion of the session establishment between the originating party and the forwarded-to party, the originating party must initiate a rekeying.

NOTE: The rekeying is designed to prevent the *forwarding party* from having the key to the bearer session associated with the originating party and the forwarded-to party. If the forwarding party had the key to the bearer session they would be able to eavesdrop on the forwarded session. LSCs, MFSS, and SS may act as a B2BUA for an EI or a AEI and would therefore originate the AS-SIP session on behalf of the EI or AEI.

o. **[Conditional: EI, AEI]** If the EI or AEI acts as a bridge or a MCU, it shall establish a unique key for each EI or AEI connection.

p. **[Conditional: EBC]** If an EBC transmits decrypted VVoIP signaling and/or bearer traffic to an external IDS/IPS, confidentiality for the decrypted signaling and media

traffic shall be ensured using cryptographic protection, where the strength of the cryptographic protocol/algorithms used is greater than or equal to the TLS and SRTP cryptographic profiles defined in this document.

q. **[Required: VPN]** At a minimum, the following confidentiality policy adjudication features shall be provided for each controlled interface. Encrypt, as needed, all outgoing communication including the body and attachment of the communication.

r. **[Required: FW, IPS, VPN]** The security device that provides remote access shall use encryption to protect the confidentiality of the session.

(1) **[Required: FW, IPS, VPN]** The security device shall provide an encrypted communication path between itself and remote administrators and authenticated proxy users that is logically distinct from the other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure.

(2) **[Required: FW, IPS, VPN]** The security device shall use encryption to provide a trusted communication channel between itself an authorized IT entity that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure.

(3) **[Required: FW, IPS, VPN]** The security device shall use a cryptographic signature to provide a communication path between itself and remote administrators and authenticated proxy users that is logically distinct from other communication paths and provides assured identification of its end points and protection.

(4) **[Required: FW, IPS, VPN]** The security device's crypto-module shall perform encryption and decryption using the AES standard. Encryption minimum is AES-128 with AES 256 as objective.

NOTE: The only exception is for SNMPv3 so that CBC-DES-128 – usmDESPrivProtocol can be supported.

s. **[Conditional: FW, IPS, VPN]** If a security device permits remote administration of its controlled interfaces, then the session must be protected through the use of strong encryption, AES 128 at a minimum.

5.4.6.2.4 Non-Repudiation

1. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of providing non-repudiation and accountability services.

   NOTE: This assumes that authentication has already occurred as required previously.

   a. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** For user-accessible resources in the product that are created or modified by a user ID via standard operations and maintenance procedures, the product shall be capable of providing a mechanism to identify the said user ID, date, and time associated with the said resource creation or modification.

   b. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of auditing at the operating system and database management system (DBMS) levels and shall have a security log that contains information to support after the fact investigation of loss or impropriety and appropriate management response.

      (1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, VPN, IPS]** The security log entry of any request or activity that is invoked by a user ID shall be capable of including that user ID so it becomes possible to establish user accountability.

      NOTE: The term user ID shall be interpreted for this requirement to include users as well as processes.

      (2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The security log shall be capable of protecting itself from unauthorized access or destruction.

         (a) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The security log protection, as a minimum, shall be capable of providing access control based on user privileges and interface (logical or physical) privileges.

         (b) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall have no mechanism for any external user (human or machine), including the administrator, to modify or delete the security log.

      (3) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The security log shall be capable of using a circular (or equivalent) recording mechanism (i.e., oldest record overwritten by newest).

(a) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS] [Alarm]** The product shall be capable of generating a security log alarm based upon specific conditions (e.g., percentage full by new entries since last upload, time interval elapsed since the last upload, disk space used). The alarm may necessitate uploading the security log (typically to some remote facility or other facility for long-term storage) to avoid an overwrite in the buffer. This upload may be automatically performed by the product or by an appropriate administrator.

(4) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** Only the system security administrator and system administrator roles shall have the ability to retrieve, print, copy, and upload the security log(s).

(a) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of ensuring security log copies maintain time sequentially and include all records stored in the security log up to the initiation of the copy.

(5) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product security log shall survive system restart (e.g. via reloading).

(6) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The security log shall be capable of recording any action that changes the security attributes and services, access controls, or other configuration parameters of devices; each login attempt and its result; and each logout or session termination (whether remote or console) to include the following events by default as a minimum:

(a) Invalid user authentication attempt.

(b) Unauthorized attempts to access system resources.

(c) Changes made in a user's security profile and attributes.

(d) Changes made in security profiles and attributes associated with a interface/port.

(e) Changes made in access rights associated with resources (i.e., privileges required of a user and a interface/port to access).

(f) Changes made in system security configuration.

(g) Creation and modification of the system resources performed via standard operations and maintenance procedures.

(h) **[Conditional]** Disabling a user profile~~.~~, if the product supports automated or manual disabling of user profiles.

(i) Events associated with privileged users.

(j) **[Conditional]** If the system contains resources that are deemed mission critical (for example a risk analysis classifies it as critical), then the system should log any events associated with access to those mission critical resources.

(k) Successful login attempts.

(l) Failed login attempts to include the following:

i. Failed login attempt due to an excessive number of logon attempts.

ii. Failed logon attempt due to blocking or blacklisting of a user ID.

iii. Failed logon attempt due to blocking or blacklisting of a terminal.

iv. Failed logon attempt due to blocking or blacklisting an access port.

(m) Account deletion or termination

(n) Changes to system time or configuration changes to the source used to establish time, such as the configured NTP server.

(7) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The security log event record shall be capable of including at least the following information:

(a) Date and time of the event (both start and stop)

(b) User ID including associated terminal, port, network address, or communication device

(c) Event type

(d) Names of resources accessed

(e) Success or failure of the event

(8) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** **[Alarm]** The product shall have the capability to notify (e.g., via critical alarm, alert, or online report), within 30 seconds, an appropriate NOC if the security log fails to record the events that are required to be recorded.

(9) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall not record actual or attempted passwords in the ~~security log~~audit log. Additionally, the audit log shall not include plaintext private or secret keys or other critical security parameters.

(10) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall ensure that security and security-related audit logs are maintained separate from other types of audit logs (history or CDR audit logs).

(11) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of transmitting all logs to a remote log server in a secure manner.

NOTE: Secure manner may be accomplished by using industry best practices to ensure the confidentiality and integrity of the logs during transfer.

(12) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product/system shall be able to generate a human understandable presentation of any audit data stored in the audit trail.

c. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** If the product accesses other systems to pass on a request or activity that has a user ID associated with it, the product shall have the capability to make that user ID available to other systems. Thus, if the other systems have the capability to accept the user ID information, the said user can be traceable for the lifetime of the request or activity.

d. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall be capable of providing post-collection audit analysis tools that can produce typical reports (e.g., exception reports, summary reports, and detailed reports) on specific data items, users, or communication facilities.

e. **[Required: MFSS, SS, LSC, MG, EBC, RSF] [Alarm]** The product shall support the capability to alert the NMS when the audit function starts up and shuts down. This capability shall be configurable.

5.4.6.2.5 Availability

1. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The VVoIP product (MFSS, LSC, etc.) shall meet the availability requirements as stated in ~~the UCR 2008,~~ Section 5.3.2~~.2.3.8~~ of this UCR, System Quality Factors~~. There are additional Information Assurance -specific Information Assurance availability requirements specified below that are not covered in the System Quality Factors section of this UCR~~.

   ~~a. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall have robustness through the maximum use of alternative routing, backup. NOTE: From a vendor's perspective this requirement is associated with meeting the reliability numbers for the product.~~

   ~~b. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall have mechanisms to allow "secure recovery" to reduce vulnerability due to failure or discontinuity making it vulnerable to security compromise.~~

   ~~NOTE: This requirement will ensure that as a system is reestablished it does not reboot in an unsecured mode such as with factory set configurations.~~

   ~~c. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall have the capability to rebuild the system to a base version and subsequent vendor modifications of that version, if that version and modification are currently in use.~~

   ~~d. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall have the capability to provide adequate check points in a process flow of the software system so that, upon detection of service deterioration, a recovery to an acceptable level is facilitated.~~

   ~~e. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The product shall have a capability to define a threshold (e.g., percentage full by new entries since last upload, time interval elapsed since last upload) to initiate a warning before a security log buffer overflow.~~

5.4.6.3 Security Device IA Requirements

1. **[Required: IPS, FW]** The security device shall support SNMPv3 and NTPv4.

2. **[Optional: FW, IPS]** The security device shall provide a true Out-of-Band-Management (OOBM) interface that will not forward to or receive from any of the routed interfaces.

3. **[Required: FW, VPN]** The security device shall provide hot standard failover capability using a proven reliability protocol.

4. **[Required: VPN]** The security device shall provide ability to push policy to the VPN Client and the ability to monitor the client's activity.

5. **[Required: VPN]** The security device shall be managed from a central place, clients, and servers.

6. **[Required: FW, IPS, VPN]** The security device shall implement NTP to ensure times are synchronized.

7. **[Required: FW]** The security device shall have three Ethernet ports, one for primary, one for backup, and one for OOBM.

5.4.6.3.1 Security Device Alarms and Alerts

This section mandates the need for security devices to inform administrators that an event has occurred.

1. **[Required: FW, IPS]** The security device shall apply a set of rules in monitoring events and based on these rules indicate a potential violation of the security device security policy.

2. **[Optional: FW, IPS, VPN] [Alarm]** Security devices with local consoles shall have the capability to generate and display an alarm message at the local console upon detection of a potential security violation.

3. **[Required: FW, IPS, VPN] [Alarm]** The security device shall have the capability to generate an alarm message to a remote administrator console upon detection of a potential security violation.

4. **[Required: FW, IPS, VPN] [Alarm]** The security device shall have the capability to generate an alarm message to a new remote administrator's console session if the original alarm has not been acknowledged following a potential security violation.

5. **[Required: IPS] [Alarm]** The security device shall have the capability to provide proper notification upon detection of a potential security violation or forward event status data to a Network Management System (NMS) that will take the appropriate action to include providing notification of the event.

6. **[Required: IPS] [Alarm]** The security device shall have the capability to immediately alert the administrator by displaying a message at the local and remote administrative consoles when an administrative session exists for each of the defined administrative roles.

7. **[Required: IPS] [Alarm]** The security device shall have the capability to provide proper notification of the audit trail exceeding a set percentage of the device storage capacity.

8. **[Required: FW, IPS, VPN] [Alarm]** The security device shall have the capability to provide a means to notify the administrator of any critical operational events (e.g., near full audit logs) within 30 seconds.

9. **[Required: IPS] [Alarm]** An automated, continuous, on-line monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any suspicious activity contrary to normal expected and recorded baseline operations.

10. **[Required: FW, IPS, VPN] [Alarm]** The security device shall have an automated, continuous online monitoring and audit trail creation capability, which shall be deployed with a user configurable capability to automatically disable the system if serious Information Assurance violations are detected.

11. **[Required: FW, IPS, VPN]** The security device shall have the capability to configure the timing of alarms and their escalation based upon type and severity of event.

5.4.6.3.2 Security Device Audit and Logging

This section requires a security device to produce records that forensics examiners can use to trace intrusions and other security events. It also mandates the records will be protected against malicious alteration.

1. **[Required: FW, IPS, VPN]** The security device shall generate an audit record of all potential security violations that are detected, complete with the identity (source and destination address) of the potential security violation, time/date, and other identifying data.

2. **[Required: FW, IPS, VPN]** The security device shall generate an audit record of each start-up and shutdown of the audit function.

3. **[Required: FW, IPS, VPN]** The security device shall generate an audit record of all modifications to the audit configuration that occur while the audit collection functions are operating to include enabling and disabling of any of the audit analysis mechanisms.

4. **[Required: FW, IPS, VPN**] The security device shall generate an audit record of any modification to the audit trail.

5. **[Required: FW, IPS, VPN**] The security device shall generate an audit record of any unsuccessful attempts to read information from the audit records.

6. **[Required: FW, IPS, VPN**] The security device shall generate an alarm or warning message upon detection of audit activity failures.

7. **[Required: FW, IPS, VPN**] The security device shall generate an audit record of all actions taken due to exceeding the audit threshold.

8. **[Required: FW, IPS, VPN]** The security device shall generate an alarm or warning message upon detection of an audit storage failure.

9. **[Required: FW, IPS]** The security device shall provide minimum recorded security relevant events including any activity caught by the "deny all" rule at the end of the security device rule base.

10. **[Required: FW, IPS, VPN]** The security device shall provide a means to store audit records to a dedicated server on the internal network.

11. **[Required: FW, IPS, VPN]** The security device shall generate an audit record of all failures of cryptographic operations.

12. **[Required: IPS]** The security device shall generate an audit record of all failures to reassemble fragmented packets.

13. **[Required: FW, IPS, VPN]** The security device shall generate an audit record of exceeding the threshold of unsuccessful authentication attempts; the actions taken (e.g., disabling of an account), and the restoration to the normal state.

14. **[Required: FW, IPS, VPN]** The security device shall generate an audit record of all use of authentication and user identification mechanisms.

15. **[Required: FW, IPS]** The security device shall generate an audit record of attempts to bind user security attributes to a subject.

16. **[Required: FW, IPS, VPN]** The security device shall generate an audit record of all modifications to the security functions of the security device.

17. **[Required: FW, IPS, VPN]** The security device shall generate an audit record of all enabling or disabling of the key generation self-tests.

18. **[Required: FW, IPS, VPN]** The security device shall generate an audit record of all modifications of the values of the security device data by the administrator.

19. **[Required: FW, IPS, VPN]** The security device shall generate an audit record of all Administrator actions and/or privileged activities.

20. **[Required: FW, IPS, VPN]** The security device shall generate an audit record of all attempted uses of the trusted channel functions.

21. **[Required: FW, IPS, VPN]** The security device shall provide the administrator with the capability to read all audit data from the audit record.

22. **[Required: FW, IPS, VPN]** The security device shall prohibit all users read access to the audit records in the audit trail, except an administrator.

23. **[Required: FW]** The security device, when configured, shall log the event of dropping packets and the reason for dropping them.

24. **[Required: FW, IPS, VPN]** The security device shall log changes to the configuration.

25. **[Required: FW, IPS]** The security device shall log matches to filter rules that deny access when configured to do so.

26. **[Required: FW, IPS, VPN]** The security device shall log hardware changes since the last maintenance cycle when configured to do so.

27. **[Required: FW, IPS, VPN]** The security device shall log new physical connections made to the security device.

28. **[Required: FW, IPS, VPN]** The security device shall prevent modifications to the audit records in the audit trail.

29. **[Required: FW, VPN]** The security device shall record access or attempted access via security device to all program initiations and shutdowns that have security implications.

30. **[Required: FW, IPS, VPN]** Audit records shall include connection attempts to the security device.

31. **[Required: FW, IPS, VPN]** The system shall create and maintain an audit trail that includes selected records of access to security-relevant objects and directories, including opens, closes, modifications, and deletions.

32. **[Required: FW, IPS, VPN]** The security device shall create an audit trail maintained by an IS that is capable of recording changes to the mechanism's list of users' formal access permissions.

33. **[Required: FW, IPS, VPN]** The security device shall record access or attempted access via controlled interfaces to objects or data whose labels are inconsistent with user privileges.

34. **[Required: FW, IPS, VPN]** The system shall create and maintain an audit trail that includes selected records of activities at the system console (either physical or logical consoles), and other system-level accesses by privileged users.

35. **[Required: FW, IPS, VPN]** The output of such intrusion/attack detection and monitoring tools shall be protected against unauthorized access, modification, or detection.

36. **[Required: FW, IPS, VPN]** Audit procedures that include the existence and use of audit reduction and analysis tools shall be implemented.

37. **[Required: FW, IPS, VPN]** Tools shall be available for the review of audit records and for report generation from audit records.

38. **[Required: FW, IPS, VPN]** Audit records shall include:

    a. User ID

    b. Successful and unsuccessful attempts to access security files

    c. Date and time of the event

    d. Type of event

    e. Success or failure of event

    f. Successful and unsuccessful log-ons

    g. Denial of access resulting from excessive number of log-on attempts

h. Blocking or blacklisting a user ID terminal or access port, and the reason for the action

i. Activities that might modify, bypass, or negate safeguards controlled by the system

j. Data required to audit the possible use of covert channel mechanisms

k. Privileged activities and other system-level access

l. Starting and ending time for access to the system

m. Security relevant actions associated with periods processing or the changing of security labels or categories of information

39. **[Required: IPS]** The security device shall log requests for access or services where the presumed source identity of the information received by the security device specifies a broadcast identity.

40. **[Required: FW, IPS, VPN]** The level of events/information audited by the security device shall be configurable.

41. **[Required: IPS]** The security device shall log SMTP traffic that contains source routing symbols (e.g., in the mailer recipient commands).

42. **[Required: FW, IPS, VPN]** The security device intrusion/attack detection and monitoring tools shall build on audit reduction and analysis tools to aid the ISSO in the monitoring and detection of suspicious, intrusive, or attack-like behavior patterns.

43. **[Required: FW, IPS, VPN]** Audit procedures shall include the capability of the system to monitor auditable events in real time that may indicate an imminent violation of security policies.

44. **[Required: FW, IPS, VPN]** A comprehensive audit trail of each remote session to include the following shall be recorded:

a. Source and destination IP addresses,

b. Connection start and end dates/times,

c. Authenticated User IDs,

d. Number of unsuccessful logon attempts before successful logon,

e. Successful and unsuccessful attempts to access system resources during remote session.

f. Privilege Escalation attempts.

g. Activities that might modify, bypass, or negate safeguards controlled by the system.

45. **[Required: IPS]** The security device shall log requests in which the information received by the security device contains the route (set of host network identifiers) by which information shall flow from the source subject to the destination subject.

46. **[Required: IPS]** The security device shall log an information flow between a source subject and a destination subject via a controlled operation if the source subject has successfully authenticated to the security device.

47. **[Required: IPS, VPN]** The security device shall log an information flow between two objects when the information security conditions match the attributes in an information flow policy rule (contained in the information flow policy database).

48. **[Required: IPS, VPN]** The security device shall log data and audit events when a user session authentication replay attack is detected.

49. **[Required: IPS, VPN]** The security device shall be able to collect the following: Start-up and Shutdown events.

50. **[Required: IPS, VPN]** The security device shall be able to collect the following: Identification, Authentication, and Authorization events.

51. **[Required: IPS, VPN]** The security device shall be able to collect the following: Data Accesses.

52. **[Required: IPS, VPN]** The security device shall be able to collect the following: Service Requests.

53. **[Required: IPS, VPN]** The security device shall be able to collect the following: Network traffic.

54. **[Required: IPS, VPN]** The security device shall be able to collect the Security configuration changes.

55. **[Required: IPS, VPN]** The security device shall be able to collect the following: Data introduction.

56. **[Required: IPS]** The security device shall be able to collect the following: Detected malicious code.

57. **[Required: IPS, VPN]** The security device shall be able to collect the following: Access control configuration.

58. **[Required: IPS, VPN]** The security device shall be able to collect the following: Service configuration.

59. **[Required: IPS, VPN]** The security device shall be able to collect the Authentication configuration.

60. **[Required: IPS, VPN]** The security device shall be able to collect the following: Accountability policy configuration.

61. **[Required: IPS, VPN]** The security device shall be able to collect the following: Detected known vulnerabilities.

62. **[Required: IPS, VPN]** The security device shall provide authorized users with the capability to read the system data.

63. **[Required: IPS, VPN]** The system shall prohibit access to security device data, except those users that have been granted explicit read access.

64. **[Required: FW, IPS, VPN]** The security device shall ensure that security device data will be maintained if the security device:

    a. Fails

    b. Is attacked

    c. Storage becomes exhausted (a circular storage method will be employed so that a Denial of Service attack could not be implemented by overloading audit trail with events.)

    d. Fails restart/reboot

65. **[Required: FW, IPS, VPN]** The security device shall have a circular log to ensure that buffers do not fill and the logging stops. They should be required to offload to external SYSLOG RAE.

66. **[Required: FW, IPS, VPN]** The security device shall be able to offload audit logs to external SYSLOG RAE.

5.4.6.3.3 Conformance Requirements

Security devices must conform to specific standards as described below:

1. **[Required: FW, IPS, VPN]** The DoD IPv6 Profile shall be used for IPv6 requirements for security devices unless otherwise stated either within this section or in UCR 2008, Section 5.3.5, IPv6 Requirements.

2. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 2409, "The Internet Key Exchange (IKE)."

3. **[Required: FW, IPS, VPN]** The security device shall conform to all of the MUST requirements found in RFC 3414, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol."

4. **[Required: FW, IPS, VPN]** The security device shall conform to all of the MUST requirements found in RFC 3412, "Message Processing and Dispatching for Simple Network Management Protocol."

5. **[Required: FW, IPS, VPN]** The security device shall conform to all of the MUST requirements found in RFC 3413, "Simple Network Management Protocol Applications."

6. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 3585, "IPSec Configuration Policy Information Model."

7. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 3586, "IP Security Policy Requirements."

8. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 4302, "IP Authentication Header."

9. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 4303, "IP Encapsulating Security Payload (ESP)."

10. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 4305, "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)."

11. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 4306, "Internet Key Exchange (IKEv2) Protocol."

12. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 4307, "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)."

13. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 4308, "Cryptographic Suites for IPSec."

14. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 4309, "Using Advanced Encryption Standard (AES) CCM Mode with IPSec Encapsulating Security Payload (ESP)."

15. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 2473, "Generic Tunneling."

16. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 4301, "Security Architecture for the Internet Protocol."

17. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 3948, "UDP Encapsulation of IPsec Packets."

18. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 3947, "Negotiation of NAT-Traversal in the IKE."

5.4.6.3.4 Security Measures

This section enumerates various measures that make the security device and its environment more secure.

1. **[Required: FW, IPS, VPN]** Passwords shall be changed at least annually employing system mechanisms that enforce current DoD password complexity policies.

2. **[Required: FW, IPS, VPN]** Passwords shall be encrypted both for storage and for transmission.

3. **[Required: FW, IPS, VPN]** The security device shall prevent the downloading of mobile code or executable content to itself.

4. **[Required: FW, IPS, VPN]** Monitoring tools shall be used for the monitoring and detection of suspicious, intrusive, or attack-like behavior patterns to itself.

5. **[Required: FW, IPS, VPN]** The security device's controlled interface shall be configured such that its operational failure or degradation shall not result in any unauthorized release of information outside the IS perimeter.

6. **[Required: FW, IPS, VPN]** DoD ISs shall comply with DoD ports, protocols, and services guidance.

7. **[Required: FW, IPS, VPN]** Where scanning tools are available, the security device's internal hosts shall be scanned for vulnerabilities in addition to the security device itself to confirm an adequate security policy is being enforced.

8. **[Required: FW, IPS, VPN]** The security device must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with security device security functions.

9. **[Required: FW]** The security device shall block unauthorized directed broadcasts from external networks (Distributed Denial of Service defense).

10. **[Required: FW]** The security device shall verify reverse path unicast addresses (Distributed Denial of Service defense) and be able to drop packets that fail verification.

11. **[Required: FW, IPS, VPN]** The security device shall drop all packets with an IPv4 non-routable (RFC 1918) address originating from an external source.

12. **[Required: FW, IPS, VPN]** The security device shall drop all packets with an IPv4 source address of all zeros.

13. **[Required: FW, IPS, VPN]** The security device shall drop all traffic from the internal network that does not use a legitimate internal address range as its source address.

14. **[Required: FW, IPS]** The security device shall differentiate between authorized and fraudulent attempts to upgrade the operating system, i.e. trying to upgrade system files with the wrong names.

15. **[Required: FW, IPS]** The security device shall differentiate between authorized and fraudulent attempts to upgrade the configuration, i.e. if a user trying to perform an upgrade that is not authorized that role.

16. **[Required: FW, IPS]** The security device shall pass traffic, which the security device has not identified as being a security problem, without altering the contents.

17. **[Required: FW, IPS]** The security device shall properly accept or deny User Datagram Protocol (UDP) traffic from port numbers based on policy.

18. **[Required: FW, IPS]** The security device shall properly accept or deny TCP traffic from port numbers based on policy.

19. **[Required: FW]** The security device shall not compromise its resources or those of any connected network upon initial start-up of the security device or recovery from an interruption in security device service.

20. **[Required: FW]** A security device shall properly enforce TCP state.

21. **[Required: FW]** A security device shall properly accept and deny traffic based on multiple rules.

22. **[Required: FW, IPS]** A security device shall prevent all known network-based current attack techniques (Common Vulnerabilities and Exploits) from compromising the security device.

23. **[Required: FW, IPS, VPN]** A security device shall prevent the currently available Information Assurance Penetration techniques, as defined in DISA STIGS and IAVAs from penetrating the security device.

24. **[Required: FW, IPS]** A security device shall block potentially malicious fragments.

25. **[Required: FW, IPS]** The security device shall mediate the flow of all information between a user on an internal network connected to the security device and a user on an external network connected to the security device and must ensure that residual information from a previous information flow is not transmitted.

26. **[Required: FW, IPS]** The security device shall not contain unauthorized compilers, editors, and other program development tools on its operational security device systems.

5.4.6.3.5 Systems and Communication Protection

These requirements enforce the security of individual systems and the communication paths.

1. **[Required: FW]** Each controlled interface shall be configured to ensure that all (incoming and outgoing) communications protocols, services, and communications not explicitly permitted are prohibited

2. **[Required: FW]** The security device's controlled interface shall ensure that only traffic that is explicitly permitted (based on traffic review) is released from the perimeter of the interconnected IS.

3. **[Required: FW]** The controlled interface is configured such that its operational failure or degradation (to include traffic load or corrupt traffic content) does not result in any unauthorized system access.

4. **[Required: FW]** The security device's controlled interface enforces configurable thresholds to determine whether all network traffic can be handled and controlled.

5. **[Required: FW, IPS, VPN]** The underlying operating system shall satisfy the confidentiality requirements of Protection Level 2 or higher, integrity requirements for Basic Level-of-Concern or higher, and availability requirements for Basic Level-of-Concern or higher.

5.4.6.3.6 Other Requirements

This section provides other functional requirements for the firewall that are not listed in previous sections.

1. **[Required: FW, IPS, VPN]** The security device shall reject requests for access or services where the presumed source identity of the source subject is an external Information Technology entity on a broadcast network.

2. **[Required: FW, VPN]** The security device shall reject requests for access or services where the presumed source identity of the source subject is an external Information Technology entity on the loopback network.

3. **[Required: FW, IPS, VPN]** The security device shall permit an information flow between a source subject and a destination subject via a controlled operation if the source subject has successfully authenticated to the security device.

4. **[Required: FW]** The TSF shall permit an information flow between a controlled subject and **another** controlled **subject** via a controlled operation if the following rules hold:

a. Subjects on an internal network can cause information to flow through the security device to another connected network if:

(1) All the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;

(2) The presumed address of the source subject, in the information, translates to an internal network address;

(3) And the presumed address of the destination subject, in the information, translates to an address on the other connected network.

b. Subjects on the external network can cause information to flow through the TOE to another connected network if:

(1) All the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;

(2) The presumed address of the source subject, in the information, translates to an external network address;

(3) And the presumed address of the destination subject, in the information, translates to an address on the other connected network.

5. **[Required: FW, IPS, VPN]** The security device, after a failure or service discontinuity, shall enter a maintenance mode where the ability to return the security device to a secure state is provided.

6. **[Required: IPS, VPN]** The security device shall detect replay attacks using either security device data or security attributes.

7. **[Required: IPS]** The security device shall reject data and audit events when a replay is detected.

8. **[Required: FW, IPS, VPN]** The security device shall ensure the security policy enforcement functions are invoked and succeed before each function within the security functions scope of control is allowed to proceed.

9. **[Required: FW, IPS, VPN]** The security device shall lock a local interactive session after a System Administrator-specified time periods of inactivity by clearing or overwriting display devices and making the current contents unreadable.

10. **[Required: FW, IPS, VPN]** The security device shall lock a local interactive session after a System Administrator-specified time period of inactivity by disabling any activity of the user's data access/display devices other than unlocking the session.

11. **[Required: FW, IPS, VPN]** The security device shall allow user-initiated locking of the user's own local interactive session by clearing or overwriting display devices and making the current contents unreadable.

12. **[Required: FW, IPS, VPN]** The security device shall allow user-initiated locking of the user's own local interactive session by disabling any activity of the user's data access/display devices other than unlocking the session.

13. **[Required: FW, IPS, VPN]** The security device shall terminate a remote session after a System Administrator-configurable time interval of session inactivity.

14. **[Required: FW, IPS, VPN]** The security device shall enforce System Administrator policy regarding Instant Messaging traffic.

15. **[Required: FW, IPS, VPN]** The security device shall enforce System Administrator policy regarding VVoIP traffic.

16. **[Required: FW, IPS, VPN]** The security device features or capabilities not required for security device operation shall be disabled to eliminate exposure to possible security vulnerabilities.

17. **[Required: FW, IPS, VPN]** Access Control shall include a Discretionary Access Control (DAC) Policy.

18. **[Required: FW, IPS, VPN]** Discretionary Access Control access controls shall be capable of including or excluding access to the granularity of a single user.

19. **[Required: FW, IPS, VPN]** The security device's controlled interface shall review incoming information for viruses and other malicious code.

20. **[Required: FW, IPS, VPN]** The controlled interface shall be configured so its operational failure or degradation (to include traffic load or corrupt traffic content) does not result in any external information entering the IS.

21. **[Required: FW, IPS, VPN]** The controlled interface shall be configured so its operational failure or degradation (to include traffic load or corrupt traffic content) does not result in any unauthorized release of information outside the IS perimeter.

22. **[Required: FW, IPS, VPN]** The controlled interface shall provide the ability to fully restore its functionality in accordance with documented restoration procedures.

23. **[Required: FW, IPS, VPN]** The security device shall prevent or mitigate DoS attacks. Where technically feasible, procedures and mechanisms shall be in place to curtail or prevent well-known, detectable, and preventable DoS attacks (e.g., SYN attack). Only a limited number of DoS attacks are detectable and preventable. Often, prevention of such attacks is handled by a controlled interface.

5.4.6.3.7 Configuration Management

This section assures the ability to administer the security device in a manner consistent with best practices. It does not mandate a specific configuration for UC devices.

1. **[Required: FW, IPS, VPN]** A CM process shall be implemented for hardware and software updates.

2. **[Required: FW, IPS, VPN]** The CM system shall provide an automated means by which only authorized changes are made to the security device implementation.

3. **[Required: FW, IPS, VPN]** The security device shall disable the Proxy Address Resolution Protocol (ARP) service, unless disabled by default.

4. **[Required: FW, IPS, VPN]** The security device shall have the capability to disable the ICMP destination unreachable notification on external interfaces.

5. **[Required: FW, IPS, VPN]** The security device shall disable IP redirection capability.

6. **[Optional: FW, IPS, VPN]** The security device shall disable the Maintenance Operations Protocol (MOP) service in DEC equipment which use that protocol to perform software loads.

7. **[Required: FW, IPS, VPN]** The security device shall be capable of shutting down any unused interfaces as determined by the administrator.

8. **[Required: FW, VPN]** The security device shall disable the service source-routing.

9. **[Required: FW, IPS, VPN]** The security device shall properly implement an ordered list policy procedure.

10. **[Required: FW, IPS]** The controlled interface shall enforce configurable thresholds to determine whether all network traffic can be handled and controlled. If a processing threshold or a failure limit has been met then the controlled interface will not continue to process transactions. These thresholds can be set to detect and defend against Denial of Service attacks such as SMURF or SYN Flood.

11. **[Required: FW, IPS]** The system administration shall employ security management mechanisms for the management of the controlled interface. This includes configuration and start/stop processing of the controlled interface. For controlled interfaces, the System Administrator may be the same as the System Administrator.

5.4.6.3.8 Documentation

This section requires documents that show a firewall was designed and implemented using best current practices. Additionally, administrative and user guides are required to ensure the firewall is delivered to sites with the documentation needed to properly secure the enclave.

1. **[Required: FW, IPS, VPN]** The developer shall provide CM documentation identifying roles, responsibilities, and procedures to include the management of Information Assurance information and documentation shall be formally documented.

2. **[Required: FW, IPS, VPN]** The developer shall provide administrator guidance addressed to system administrative personnel (e.g., Administrator's Guide).

3. **[Optional: FW, IPS, VPN]** The developer shall provide user guidance (e.g., User's Guide) when there are users other than administrators. The User's Guide will describe the protection mechanisms provided, guidelines on how the mechanisms are to be used, and the ways the mechanisms interact.

4. **[Required: FW, IPS, VPN]** The developer shall provide the architectural design of the security device.

5. **[Required: FW, IPS, VPN]** The developer shall provide a functional specification of the security device.

6. **[Required: FW, IPS, VPN]** The developer shall perform strength of security device analysis for each mechanism identified in the Security Target as having strength of security device claim.

7. **[Required: FW, IPS, VPN]** The developer shall provide an analysis of the test coverage.

8. **[Required: FW, IPS, VPN]** The developer shall provide covert channel analysis documentation identifying any covert channels detected along with alternative strategies for mitigating any associated vulnerabilities.

9. **[Required: FW, IPS, VPN]** The developer shall provide vulnerability analysis documentation identifying known security vulnerabilities regarding the configuration and use of administrative functions. The vulnerability analysis documentation shall also describe the analysis of the security device deliverables performed to search for obvious ways in which a user can violate the security device security policy.

10. **[Required: FW, IPS, VPN]** The reference document for the security device shall be unique to each version of the security device.

11. **[Required: FW, IPS, VPN]** The security device shall be labeled with its reference information i.e. model and version number.

12. **[Required: FW, IPS, VPN]** The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

13. **[Required: FW, IPS, VPN]** The CM system shall provide measures such that only authorized changes are made to the configuration items.

14. **[Required: FW, IPS, VPN]** The guidance documentation shall list all assumptions about the intended environment.

15. **[Required: FW, IPS, VPN]** The system shall demonstrate a procedure for accepting and acting upon user reports of potential security flaws and requests for corrections to those flaws.

16. **[Required: FW, IPS, VPN]** The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the security device.

17. **[Required: FW, IPS, VPN]** The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

18. **[Required: FW, IPS, VPN]** The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

19. **[Required: FW, IPS, VPN]** The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections, and guidance on corrective actions to security device users.

20. **[Required: FW, IPS, VPN]** The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to security device users.

21. **[Required: FW, IPS, VPN]** The developer shall perform a vulnerability analysis.

22. **[Required: FW, IPS, VPN]** The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.

23. **[Required: FW, IPS, VPN]** The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the security device.

24. **[Required: FW, IPS, VPN]** The vulnerability analysis documentation shall justify that the security device, with the identified vulnerabilities, is resistant to obvious penetration attacks.

25. **[Required: FW, IPS, VPN]** The installation, generation, and start-up documentation shall describe all the steps necessary for secure installation, generation, and start-up of the security device.

26. **[Required: FW, IPS, VPN]** The administrator guidance shall describe recovery procedures and technical system features to assure that system recovery is done in a trusted and secure manner.

27. **[Required: FW, IPS, VPN]** The developer shall provide a statement about the source country for each software module/capability within the device.

5.4.6.4 Smartphone End Instrument and Backend Support Requirements

1. **[Conditional: EI, AEI]** If the system is a "Smartphone End Instrument," defined as an EI or AEI application that operates on an advanced mobile computing platform providing functions and features beyond basic telephony, the device shall comply with the subtended

requirements.

NOTE: The “advanced mobile computing platform” could be any portable electronic device as defined in 8100.2 to include commercial smartphones, wireless tablets or “slates,” electronic pads, small form factor notebooks, etc.

a. **[Required: Smartphone_EI]** The platform on which the Smartphone EI is utilized shall comply with all of the requirements contained in applicable STIGs, STIG Checklists, and other DISA FSO Publications to include Security Requirements Matrices.

(1) **[Required: Smartphone_EI]** The requirements related to protection of data-at-rest shall also apply to sensitive information utilized by the VVoIP application. This includes call history, phone book, contacts, directory information, and any other VVoIP application related records.

(2) **[Required: Smartphone_EI]** The product shall comply with all of the requirements in the DISA FSO "Smartphone Security Requirements Matrix."

(3) **[Conditional: Smartphone_EI]** If the platform on which the Smartphone EI resides supports e-mail, web browsing, and other services, these services shall be in accordance with all applicable STIGs, STIG Checklists, and other DISA FSO Publications to include Security Requirements Matrices

b. **[Required: Smartphone_EI]** The Smartphone EI application shall comply with all of the requirements contained in applicable STIGs, STIG Checklists, and other DISA FSO Publications to include Security Requirements Matrices.

c. **[Required: Smartphone_EI]** The Smartphone EI application shall conform to all of the requirements specified for EIs or AS-SIP EIs (as appropriate) in this UCR, with the exception of the following requirements:

(NOTE: This includes and is not limited to the capability to establish precedence calls from the Smartphone EI, support precedence rings, display caller ID and precedence level information, and support operation on IPv6 enabled Smartphone EI platforms and networks.)

(1) **[Conditional: Smartphone_EI]** If the Smartphone EI does not support all of the codec types specified in Section 5.3 for EIs and AEIs, this non-compliance is permitted, provided that the Smartphone EI SBSS transcodes appropriately when communicating with the LSC (or MFSS or SS); thereby maintaining

interoperability with normal EIs and AEIs that do support these codecs.

NOTE: This requirement is intended to accommodate bandwidth constrained wireless networks where codecs such as G.711 may consume too much bandwidth.

d. **[Required: Smartphone_EI]** All and media (e.g. voice) transmitted from the Smartphone EI application shall be protected using encryption and integrity mechanisms that are validated as conforming to FIPS 140-2 requirements.

(1) **[Required: Smartphone_EI]** The cryptographic profile (algorithms used for confidentiality, integrity, etc.) utilized to establish secure connectivity from the Smartphone EI to the SBSS shall be equal to or stronger than the profiles specified for the TLS and IPSec in Section 5.4 of this UCR for data and signaling information. For VVoIP media traffic, the cryptographic profile shall be equal to or stronger than the profile defined for SRTP in Section 5.4 of this UCR.

e. **[Conditional: Smartphone_EI]** If the Smartphone EI is operated on a platform that supports the receipt of calls from the PSTN, the application shall prevent incoming calls received via the PSTN from interrupting calls made using the Smartphone EI's homed LSC.

NOTE: Acceptable behavior in this case includes sending the PSTN call to voicemail or briefly notifying the user of the incoming call without tearing down the VVoIP session with the LSC.

f. **[Conditional: Smartphone_EI]** If the Smartphone EI supports the capability to establish and receive PSTN calls, the Smartphone EI shall support the capability to alert the user when an incoming call is received from the homed LSC (or MFSS or SS), during active calls to the PSTN.

g. **[Required: Smartphone_EI]** The Smartphone EI shall support the capability to establish a mutually authenticated, secure connection to the SBSS which utilizes X.509v3 certificates from a DoD approved PKI for validation of the SBSS and the Smartphone EI.

(1) **[Required: Smartphone_EI]** The Smartphone EI shall perform all of the certificate validation and revocation checks specified in Section 5.4 when establishing the mutually authenticated, secure connectivity to the SBSS.

h. **[Required: Smartphone_EI]** The Smartphone EI shall support the capability to utilize a CAC to authenticate a user to the Smartphone EI application. This capability shall be configurable.

NOTE: If the underlying platform already requires the use of a CAC to enable to the device, then it is permitted for the Smartphone EI to leverage the results of this authentication process if accessible to the application.

i. **[Required: Smartphone_EI]** Smartphone EIs that provide an 802.11 WLAN capability or connect to DoD-owned WLAN networks shall comply with all of the requirements applicable to Wireless End Instruments (WEIs) specified in Section 5.3 of this UCR.

j. **[Conditional: Smartphone_EI]** If the Smartphone EI also supports an instant messaging capability, that capability shall be in accordance with Section 5.7 of this UCR and any applicable STIGs and STIG checklists (to include the Instant Messaging STIG).

k. **[Objective: Smartphone_EI]** If the device is locked, possibly in a lower power state, but not powered off, the Smartphone EI shall provide users the capability to continue to receive calls from its homed LSC or SS, via the SBSS, while in this state.

NOTE: The goal of this requirement is to ensure that the device does not require the user have the device unlocked and fully active (e.g. display on at full power, all components fully active) in order to receive calls and to facilitate better battery life for Smartphone EI.

2. **[Required: SBSS]** The Smartphone Backend Support System (SBSS) shall provide secure connectivity to the LSC (or SS or MFSS) on behalf of any served, securely connected Smartphone EIs, while maintaining or enhancing the security posture of the network.

a. **[Required: SBSS]** The system shall comply with all of the requirements contained in applicable STIGs, STIG Checklists, and other DISA FSO Publications to include Security Requirements Matrices for all voice, e-mail, web-browsing, instant messaging, or any other service provided.

(1) **[Required: SBSS]** The system shall at minimum support all of the remote administration commands (remote wipe, remote disable, etc.) specified in the applicable STIGs and FSO Security Requirements matrices for any remotely supported Smartphone EIs.

b. **[Required: SBSS]** On the interface used by the SBSS to communicate with its homed LSC or SS, the SBSS shall act as any other EI or AEI and therefore comply with all of the applicable requirements in this UCR for EIs or AEIs as appropriate.

(1) **[Required: SBSS]** If the VVoIP media traffic transmitted between the Smartphone EI and the SBSS does not use one of the codecs required in Section 5.3 of this UCR, the system shall support a transcoding function that translates this media traffic accordingly in a secure manner.

(2) **[Required: SBSS]** The system shall mark traffic associated with VVoIP media, signaling, instant messaging, e-mail, web browsing, and any other supported service with the appropriate DSCP value specified in Section 5.3 on the interface used to communicate with the homed LSC or SS.

c. **[Required: SBSS]** The system shall ensure separation is maintained between concurrent sessions transiting the system.

d. **[Required: SBSS]** The system shall provide a secure connectivity by at a minimum implementing Back-to-Back User Agent (EBC-like) application layer gateway functionality or VPN termination functionality.

(1) **[Required: SBSS]** The data transiting within and external to the system shall remain encrypted at all points with cryptographic strength consistent with the TLS and IPSec profiles or SRTP profile (for media) specified in UCR Section 5.4. The system must not rely on physical safeguards alone to provide confidentiality for data in transit.

(2) **[Required: SBSS]** The system shall utilize X.509 certificates from a DoD approved PKI in accordance with the validation and revocation requirements specified in Section 5.4, to support the establishment of a mutually authenticated connection to authorized Smartphone EIs.

(3) **[Required: SBSS] [Alarm]** The system shall only permit access by only authorized Smartphone EIs. The system shall alert the NMS if it detects attempted connections from unauthorized Smartphone EIs or large numbers of failed connectivity attempts.

e. **[Required: SBSS]** The portions of the SBSS which establish secure connectivity to the Smartphone EI and other security critical components of the SBSS (specifically any portions of the SBSS that provide functionality equivalent to devices specified in existing protection profiles including FWs, IDSs, and VPNs) shall be NIAP validated.

NOTE: The system can utilize/incorporate already NIAP validated components in a secure manner to comply with this requirement.

f. **[Objective: SBSS]** The system shall provide a number portability and call forwarding feature. This capability shall allow users that travel outside of the enclave to utilize the same profile and phone number, associated with their assigned EI or AEI within the enclave, but on their Smartphone EI.

5.4.7 Quality Assurance Provisions

5.4.7.1 Responsibility for Inspection

The responsibility for inspection of the requirements is assigned to one of two organizations depending on whether the satisfaction of the requirement is related to interoperability. If the requirement is an interoperability issue then the JITC will test the system to ensure that the requirement has been met and is interoperable through the Telecom Switched Services Interoperability (TSSI) Program. The TSSI program includes interoperability certification of the DoD's voice, video, and data services. Regardless of whether the requirement has an interoperable aspect, the Information Assurance Test Team (IATT) will conduct an Information Assurance assessment of the system to ensure that all Information Assurance requirements are satisfied in accordance with the ~~VVoIP~~ UC Information Assurance Test Plan (IATP) and the appropriate STIGs. Due to constantly evolving security threats, the IATP is also used to test Information Assurance related aspects of a solution that are not mandated by requirements.

The UCCO has the responsibility for the coordination of all testing, both Information Assurance and interoperability. The IATT is part of the JITC and is sponsored by the DISA Office for Information Assurance engineering and the DSN PM. The IATT reports the test results of the Information Assurance assessment to the DISA FSO. The FSO is responsible for writing a recommendation to the DISN Security Accreditation Working Group (DSAWG), in coordination with the CA who signs the DSAWG recommendation letter. The DSAWG is the organization which makes the final decision to accept any residual risks associated with the system before its Information Assurance certification and accreditation. Once the system receives DSAWG accreditation and JITC interoperability certification, it is placed on the APL. The details of the IATP can be found on the JITC TSSI Web site (http://jitc.fhu.disa.mil/tssi/index.html) and the details of the STIGs can be found on the DISA FSO website (http://iase.disa.mil/stigs/stig/index.html).

Once an APL product is procured and installed at a location, it shall comply with the appropriate STIGs and shall report its status to the appropriate Single System Manager (SSM) annually. It is imperative that the system configuration is consistent with the configuration used during the APL process. Upon installation, the Information Assurance configuration settings must be

validated as part of the DIACAP as described in the Interim Department of Defense (DoD) C&A Process Guidance to attain its C&A, ATO, and/or its ATC. Subsequently, these system settings and Information Assurance posture must be reviewed and revalidated annually as part of the annually status update to the appropriate SSM. In addition, the product must be kept up to date with any relevant Information Assurance Vulnerability Management (IAVM) notices. This is usually accomplished by installing security patches that are tested, verified, and distributed by the vendor and/or by upgrading to the latest software or operating system release that is certified and approved for installation.

The DIACAP process includes the generation of a System Security Authorization Agreement (SSAA). SSAAs are written to cover a single product or an entire enclave that encompasses multiple products. The SSAA documents details of the system/enclave architecture, configuration, physical security and operating environment, security settings, users, owners, Information Assurance personnel, threats, vulnerabilities, mitigations, and Information Assurance requirements for the product or system. The SSAA is a living document for the lifecycle of the system and is updated as modifications are made to the system/enclave or as its Information Assurance posture changes. The DIACAP process is the responsibility of the Information Assurance personnel (DAA, IAM, IAO, and system administrators) at the site where the system is installed. A download link to a "DSN Site SSAA Template" can be found at the bottom of the following web page: http://www.disa.mil/gs/dsn/ia_canda.html. The type of template(s) is determined by the types of services provided at the site.

The APL C&A and APL listing is not a replacement for DIACAP and local instantiation C&A. Listing on the APL states that the product, in the configuration that was presented for testing, is capable of meeting DoD requirements for Information Assurance and interoperability, and is therefore able to be purchased by DoD components. The DIACAP on the other hand is necessary to validate and document that the product is properly installed and meets all relevant Information Assurance requirements before it is allowed to operate with or connect to the DISN. Annual reviews and revalidation is necessary to validate and document that the products and systems are being operated in compliance with the Information Assurance requirements and remains secure.

5.4.8 Mitigated Risks

The VVoIP Information Assurance Architecture is designed to mitigate the Information Assurance risks associated with the VVoIP architecture. This goal was accomplished using a combination of commercial "best practices" and DoD unique approaches that are consistent with DoD policies and instructions. The result of this effort was the documentation of a set of requirements for the different appliances used within the DoD VVoIP environment. Based on the requirements, in combination with the VVoIP Information Assurance Architecture, and in the knowledge that this UCR 2008 complements the STIGs, the Information Assurance threats associated with the VVoIP environment have been adjusted to reflect the mitigated risk and the

results are shown in Tables 5.4.8-1 through 5.4.8-8. It is understood that in most cases, the impact of the attack remains constant and the mitigation efforts are mainly focused on reducing the likelihood of the attack.

Table 5.4.8-1. Adjusted General Threat Risk Assessment

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G1	Eavesdropping on VVoIP subscriber transport data	1	2	2	The use of SRTP with AES 128 mitigates likelihood to a 1. In addition, the rekeying of a call transferred session mitigates this threat.
G2	Corruption of transport data	1	3	3	The use of an SHA-1 hash mitigates the likelihood of this attack to a 1.
G3	Eavesdropping on a valid telephone number to determine its location or to masquerade	1	3	3	The use of AS-SIP with TLS (or its equivalent) for all signaling sessions mitigates the likelihood to a 1.
G4	Eavesdropping on the signaling data	1	3	3	The use of AS-SIP with TLS (or its equivalent) for all signaling sessions mitigates the likelihood to a 1.
G5	Corruption of signaling data via malformed packets or protocol fuzzing	1	3	3	The use of TLS with SHA-1 mitigates the likelihood to a 1.
G6	Eavesdropping on network management traffic	2	1	2	The use of SNMPv3, SSHv2, SSLv3.1, or TLSv1.0 with 128 bit encryption mitigates this risk. The reason why the likelihood was not reduced to a 1 is that many vendors cannot implement SNMPv3 and in addition it is possible other NM protocols, like TFTP, will still be used in the architecture.
G7	Corruption of network management data	1	3	3	The use of SHA-1 for SNMPv3, SSHv2, SSLv3.1, or TLSv1.0 reduces the likelihood of this type of attack. At this time, these are the only network management protocols defined for the VVoIP architecture

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G8	Obtaining telephone number from VVoIP end instrument	1	2	2	The elimination of remote configuration and the use of a PIN (User ID) and password (2nd PIN) for configuration reduce the likelihood of this attack to a 1.
G9	Denial of service	2	2	4	This type of attack is one of the most difficult to mitigate. However, the use of VLANs in combination with filtering and traffic conditioning limit the impact this attack. In addition, appropriate network management and authentication limits the likelihood of this type of attack.
G10	Unauthorized access to data	1	3	3	The requirements associated with this type of attack such as access controls based on user profiles and the requirements associated with authentication limit this attack.
G11	Flooding the network	2	2	4	Similar reasons to DoS attacks.
G12	Stolen terminals	1	3	3	The use of CRL or OSCR in combination with user authentication for above ROUTINE precedence sessions mitigates the likelihood of this attack. Another consideration is that if the terminal is in a high risk environment (forward deployment), it is possible to require user authentication for any session, to include ROUTINE. Finally, the use of network management capabilities (Code Block) in combination with the ability to disable individual terminals also mitigates the likelihood to a 1
G13	Subscription or toll fraud	2	1	2	The implementation of authentication in combination with non-repudiation limits the likelihood of this attack
G14	Unauthorized access to network management or subscriber database	1	3	3	The limiting of access to the database to authenticated and authorized personnel in addition to the database IA requirements mitigates the likelihood of this type of attack.

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G15	Unauthorized access to data in end instruments	1	1	1	The elimination of remote configuration and the use of a User ID (PIN) and password (2nd PIN) for configuration reduce the likelihood of this attack to a 1. In addition, the compliance of the EI and AEI with FIPS 140-2 also reduces the likelihood of this attack.
G16	Masquerading as one legitimate subscriber or signaling device to another	1	3	3	The use of mutual authentication for signaling appliances reduces the likelihood of this attack. In addition, the authentication of the EI and AEI to the LSC also reduces the likelihood of this type of attack.
G17	Man-in-the-middle attack	1	3	3	The use of 128-bit encryption for all session streams in combination with authentication and traffic segmentation (VLANs, filtering, etc.) reduces the likelihood of this type of attack to a 1.
G18	Repudiation of actions	1	2	2	The logging of information and the requirements associated with the storage of logged information reduces the likelihood of this type of attack. In addition, the authentication of appliances and users facilitates the rapid detection of a malicious user.
G19	Replay Attack	1	2	2	The integrity mechanisms required by the system mitigate the likelihood of this attack.
G20	SIP Parser Attack	1	2	2	The requirement to authenticate and the hardening of the EIs and SIP signaling should mitigate the likelihood of this attack.
G21	SIP Registration or INVITE Flooding – DoS Attack	1	3	3	The requirement to authenticate and the hardening of the EIs and SIP signaling appliances should mitigate the likelihood of this attack. This is primarily an insider attack threat and the defense in depth strategy should make this an easily detected and isolated attack.

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G22	Buffer Overflow Attack	1	3	3	The likelihood of this attack is small due to the requirement to mutually authenticate all signaling appliances. This attack is associated with malformed SIP messages causing the buffer to overflow.
G23	SIP INVITE	2	1	2	The SIP timers should clear this issue within approximately 32 seconds. In addition, this attack would only affect one phone at a time.
G24	SPAM over Internet Telephony (SPIT)	1	2	2	This attack would have to originate within the SBU voice due to the TDM constraint to the PSTN.
G25	Worms, Viruses, and Trojans	1	3	3	Remove applications that are not VVoIP related from VVoIP appliances. Install antivirus software on appliances that have applications.
G26	Exploitation of a "zero-day" vulnerability	2	2	4	Mitigated by requiring vendors to state the extent of their security liability within product warranties. Reputable vendors are utilized, who specify framework/details for expeditious security fixes throughout a period as specified/agreed to by the Government. Vendors should (1) conduct reviews of their components, inspecting for any security issues and (2) correct any issues expeditiously upon detection. Government processes provide timely implementation of available fixes through CERT coordination/IAVA response, secure configuration management policies/procedures, etc. Underlying/complementary defense-in-depth safeguards further lower the probability and impact of occurrence.

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G27	Disabling of security controls by authorized users.	1	3	3	Controls to prevent (hardening, authorization, limited accounts) detect (audit/monitor), and/or respond (defense-in-depth, compensating controls, manual/automatic resets) to security control circumvention lower the likelihood to a 1.
G28	Exploitation of numerous vendor-specific VVoIP product vulnerabilities	1	2	2	See notes for G26. The likelihood is lower due to this category addressing existing vulnerabilities.
G29	Exploitation of underlying (i.e., not VVoIP-specific) network and/or system vulnerabilities	1	2	2	Integration and compliance with the DODI 8500.2 baseline controls will largely mitigate this risk through layers of defense-in-depth safeguards.
G30	Unintentional flooding	2	2	4	End point safeguards to mitigate risk include: appropriate configuration designations (e.g., IP phones with sufficient registration interval duration); vendor warranties/fixes (see G26) for component malfunctions that cause flooding; and power-related protection (e.g., UPS, etc) to protect against flooding due to simultaneous end point registration after a power outage.
G31	Security devices collectively impact QoS.	1	2	2	Performance requirements are included in the UCR to ensure appropriate QoS.
G32	Components within the system from untrusted sources could serve as future attack points, such as back doors, logic bombs, etc.	1	2	2	See G26 notes. Purchasing from reputable vendors, who conduct internal product reviews/inspections and warranty against defect (including security-related issues), provides for adequate mitigation.

Table 5.4.8-2. Data Deletion Threat Risk Assessment

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
D1	Eavesdropping of old address	2	1	2	The use of NAT may mitigate the likelihood of this attack.
D2	Masquerading as a subscriber to delete data	1	3	3	The limiting of access to the database to authenticated and authorized personnel in addition to the database IA requirements mitigates the likelihood of this type of attack.

Table 5.4.8-3. Subscriber Registration Threat Risk Assessment

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
SR1	Illegal registration by an attacker masquerading as a voice or video switch/appliance	1	1	1	The use of mutual authentication for signaling appliances reduces the likelihood of this attack. In addition, the authentication of the EI and AEI to the LSC also reduces the likelihood of this type of attack.

Table 5.4.8-4. Subscriber De-Registration Threat Risk Assessment

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
SD1	Illegal de-registration by an attacker masquerading as a voice or video switch/appliance	1	1	1	The requirements associated with authentication of a system before processing commands may mitigate the likelihood of this type of attack.
SD2	Subscriber does not allow de-registration by manipulating the end instrument	2	1	2	The impact is minimal since the subscriber should be easily isolated using firewalls and other security mechanisms such as authentication of the EI and AEI to the LSC, the use of User ID (PIN) and password (2nd PIN) for the configuration of the EI and AEI, and the encryption of network management.

SD3	Subscriber does not allow de-registration by manipulating VVoIP server	1	3	3	The requirements for authentication and authorization of a user on the system mitigate the likelihood of this type of attack. In addition, the requirements associated with hardening the system and ensuring the integrity of the system also mitigates the likelihood of this type of attack.

Table 5.4.8-5. Incoming Call Threat Risk Assessment

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
I1	Masquerading by using someone's ID	1	2	2	Since authentication is mandatory the likelihood is low.
I2	Masquerading by using someone's ID and authentication	1	3	3	The design of the authentication mechanism should be sufficient to minimize the likelihood of an attack. However, if the mechanism is broken it makes a large segment of the network vulnerable.
I3	Eavesdropping of the communication on the access interface by use of a session key	1	2	2	There are many requirements in the system associated with the protection of the session key to include the FIPS-140-2 compliance requirements that mitigate the likelihood of this threat In addition, session keys have a shorter lifespan than the time it should take to break the key. The key is not sent in the clear making it difficult to obtain.
I4	Eavesdropping of the start of a communication on the end instrument	1	1	1	This threat is mitigated by completing authentication of the session before the session is established in combination with completing the distribution of the session key before the session is established.
I5	Modification of routing data	1	3	3	This is mitigated by requiring mutual authentication between routing appliances in combination with the encryption and applying integrity checks to the routing packets.
I6	Message alteration: call black holing	1	3	3	Safeguards protect unauthorized changes to intermediary device configurations, including authentication and access controls. Signaling streams that traverse the appliance and its Assured Services Local Area Network (ASLAN) are encrypted using SIP/Transport Layer Security (TLS).

Table 5.4.8-6. Outgoing Call Threat Risk Assessment

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
01	Masquerading using a subscriber's ID	1	2	2	This attack is associated with outgoing calls and the likelihood is minimized if authentication is required.
02	Masquerading using a subscriber's ID and authentication	1	3	3	There are many policies and procedures established in the DoD that address how one must protect their passwords. This UCR 2008 does not address those policies and procedures.
03	Eavesdropping on the access interface by using a session key	1	2	2	There are many requirements in the system associated with the protection of the session key to include the FIPS-140-2 compliance requirements that mitigate the likelihood of this threat In addition, session keys have a shorter lifespan than the time it should take to break the key. The key is not sent in the clear making it difficult to obtain.
04	Eavesdropping on the network	1	3	3	The use of encryption for all layers should minimize the likelihood of this event occurring.
05	Eavesdropping on the start of a communication on the end instrument	1	1	1	This threat is mitigated by completing authentication of the session before the session is established in combination with completing the distribution of the session key before the session is established
06	Eavesdropping on the phone number of a called party	1	1	1	This threat is mitigated by completing authentication of the session before the session is established in combination with completing the distribution of the session key before the session is established.
07	Modification of the dialed number	1	3	3	This threat is mitigates by the use of authentication by appliances and users (for above ROUTINE precedence sessions) in combination with encryption and integrity checks for all sessions

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
08	Masquerading using someone's ID	1	1	1	This is not allowed since authentication is required before allowing a session to be established

Table 5.4.8-7. Emergency and Precedence Call Threat Risk Assessment

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
E1	Misuse of emergency call	2	1	2	The use of non-repudiation does not prevent this type of attack, but does allow for the rapid discovery of the malicious user or EI and AEI
E2	Misuse of precedence calls	1	3	3	This threat is mitigated by the requirements associated with user authentication and EI and AEI authentication for above ROUTINE level sessions
E3	Manipulation of emergency database information	1	3	3	The requirements associated with user authentication and authorization for database access decrease the likelihood of this type of attack.
E4	Manipulation of precedence database information	1	3	3	The requirements associated with user authentication and authorization for database access decrease the likelihood of this type of attack.

Table 5.4.8-8. Survivability Threat Risk Assessment

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
S1	A node in the network is destroyed or disabled	3	1	3	The requirements associated with survivability such as dual homing, FFR, backup power, COOP requirements, standalone capabilities reduce the impact of this attack
S2	A device in the network is disabled or destroyed	3	1	3	The requirements associated with survivability such as dual homing, FFR, backup power, COOP requirements, standalone capabilities reduce the impact of this attack

As discussed in the earlier threat section, the threats are defined as critical, major, and minor according to the product of their likelihood of an attack being successful score and the impact of a successful attack score as shown in Figure 5.4.8-1.

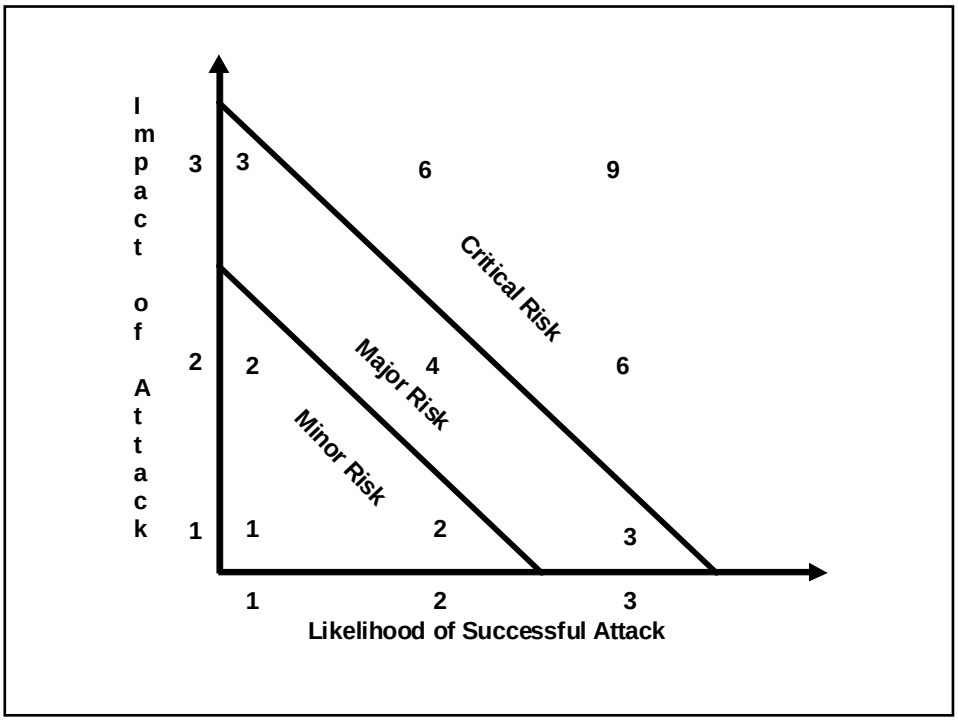

Figure 5.4.8-1. ETSI TIPHON Threat Risk Score

Based on the mitigations discussed in UCR 2008, all of the critical risk threats have been mitigated to a major risk or below category. In addition, many of the major risk threats have been mitigated to a lower score or have been reduced to a minor risk. Table 5.4.8-9, Adjusted Risk Summary, tabulates the results of the risk mitigation effort.

Table 5.4.8-9. Adjusted Risk Summary

RISK LEVEL	NUMBER OF RISKS (BEFORE MITIGATION)	NUMBER OF RISKS (AFTER MITIGATION)
Critical Risks	27	0
Major Risks	16	31
Minor Risks	15	27
Total	**58**	**58**

THIS PAGE INTENTIONALLY LEFT BLANK